Proof of Concept (PoC) Report: Ransomware Decryption Tools

Intern Name: Prajwal Sharma

Internship ID: 402

Date: July 2025

1. Executive Summary

This Proof of Concept (PoC) report evaluates the functionality and utility of two critical cybersecurity tools: the Thanatos Decryption Tool and the ThunderX Decryptor. These tools are designed to aid in the recovery of files encrypted by their respective ransomware variants, thereby mitigating financial loss and operational disruption for victims. The report outlines their historical context, core functionalities, operational workflows, and key features, including batch decryption capabilities, ransomware strain detection, and comprehensive logging. Through visual evidence and detailed descriptions, this document demonstrates the effectiveness of these decryptors in real-world scenarios, highlighting their significance in digital forensics, incident response, and business continuity planning. While highly effective for supported variants, areas for future improvement include broader variant coverage and enhanced user interfaces.

2. Tool Overview

This report focuses on two specialized digital forensics solutions:

- **Thanatos Decryption Tool**
- **ThunderX Decryptor**

These tools are specifically engineered to restore files encrypted by their respective ransomware strains by scanning for affected files, validating the ransomware strain, and executing decryption using specific algorithms or extracted keys.

2.1. History of Ransomware Variants

- **Thanatos Ransomware:** This variant appeared in early 2018. It was notable for exploitable flaws in its encryption implementation, which allowed for free decryption for some victims. Cybersecurity communities, including initiatives like NoMoreRansom, subsequently developed and published decryption tools to assist those affected.
- **ThunderX Ransomware:** This is a lesser-known variant for which specialist decryptors were released following reverse engineering efforts and collaborative cybersecurity research.

2.2. Purpose of These Tools

- **Thanatos Decryption Tool:** Facilitates the recovery of files encrypted by Thanatos ransomware via cryptanalysis and key search. Users benefit significantly by recovering their data without engaging in ransom negotiations with criminals.
- **ThunderX Decryptor:** Empowers victims of ThunderX attacks to regain access to their encrypted files. This is achieved by leveraging community-shared keys or identified code weaknesses by security researchers.

3. Key Characteristics and Features

- Targeted decryption of Thanatos/ThunderX ransomware-encrypted files
- Support for both batch processing for large numbers of files and individual file decryption
- Simple interface (Command Line Interface or Graphical User Interface, depending on the specific tool version)
- Capability for log and report generation detailing session actions
- Compatibility with Windows operating systems
- Most versions are open-source and maintained by the cybersecurity community

Modules/Types Available:

Module/Type	Function
Batch File Decryption	Processes large numbers of encrypted files
Strain Detection	Verifies if files match supported ransomware
Automated/Manual Decryption	Offers options depending on the tool's design
Logging & Export	Generates detailed logs and results summaries

4. Benefits of Using These Tools

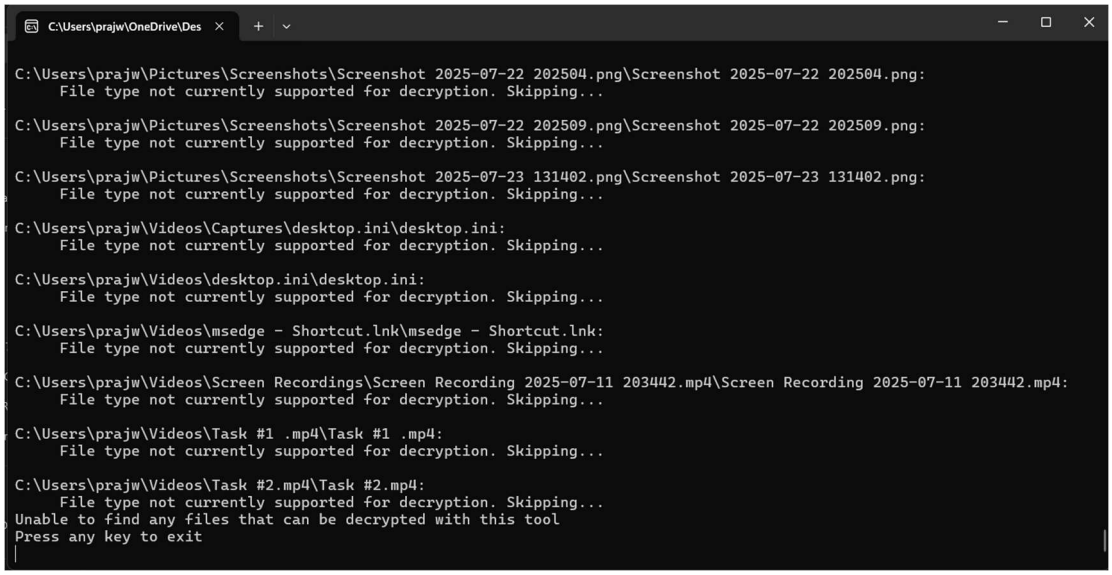
These tools offer significant advantages in ransomware incident response:

- **Cost-Effective Recovery:** They restore access to files without the need for ransom payments.
- **Digital Forensics Support:** They aid digital forensics and post-incident investigations by providing mechanisms for file recovery and analysis.
- **Compliance & Audit:** They facilitate the generation of evidence and audit logs essential for compliance requirements.
- **Minimizing Downtime:** They help organizations minimize operational downtime and data loss following a ransomware attack.

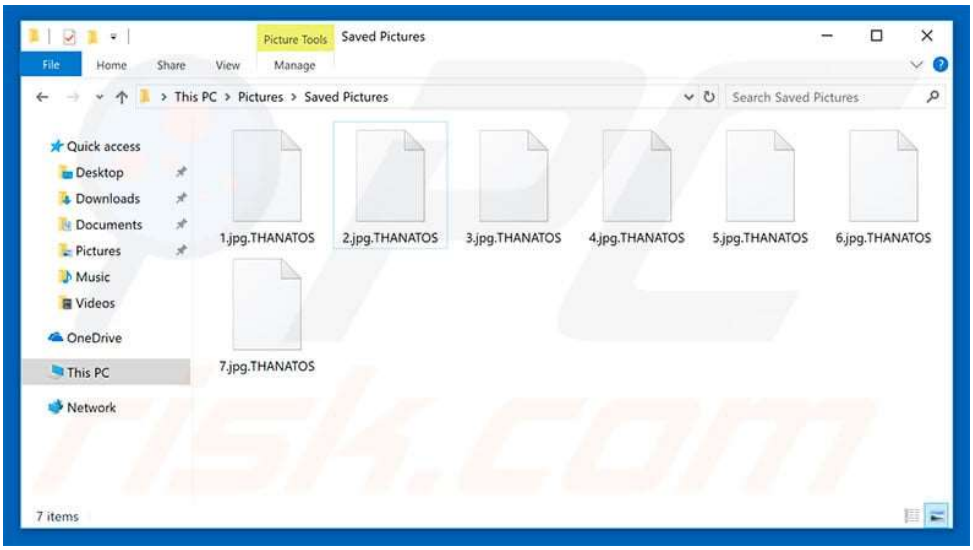
5. Proof of Concept: Visual Walkthrough

This section provides visual evidence of the decryption tools in action, demonstrating their operational aspects and results in various scenarios.

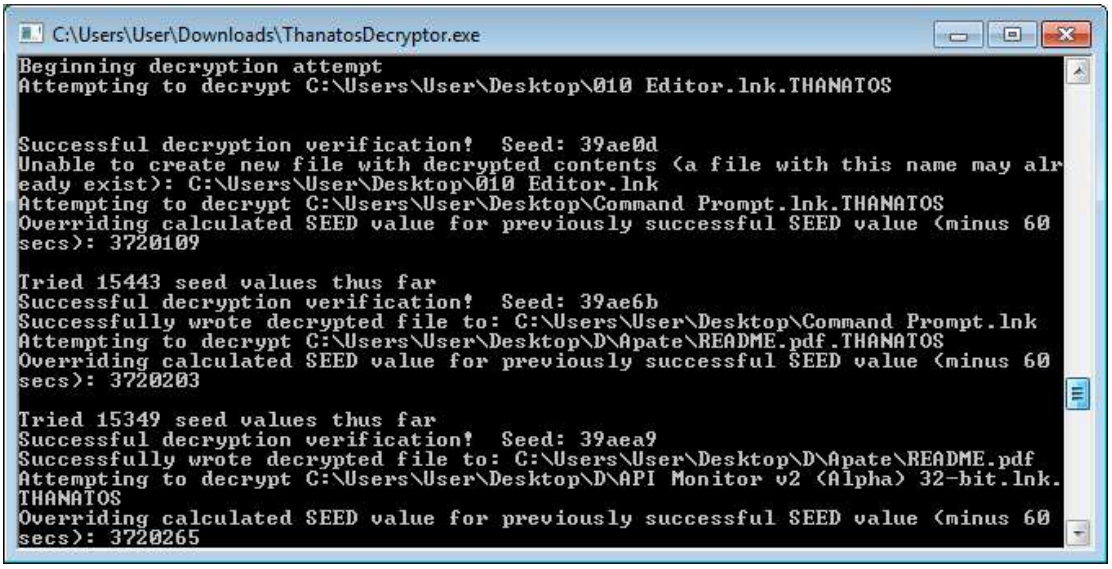
5.1. Thanatos Decryption Tool in Action



This screenshot displays a typical command-line interface of the Thanatos Decryption Tool during a ransomware investigation. It shows the tool scanning directories and attempting decryption. Messages such as "File type not currently supported for decryption. Skipping..." indicate files that the tool cannot process, which helps document its limitations and the overall outcome of the decryption attempt.

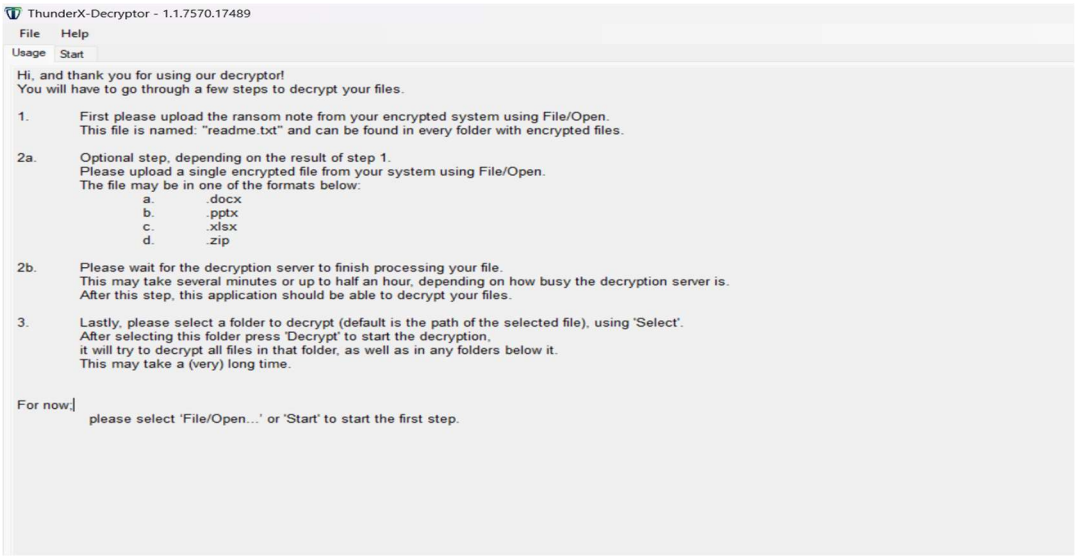


This example illustrates a folder containing multiple files that have been encrypted by Thanatos ransomware, now bearing the `.THANATOS` extension. This visual proof is crucial for demonstrating the state of encrypted files before the decryptor is used, and can be paired with "after" screenshots to show successful restoration.

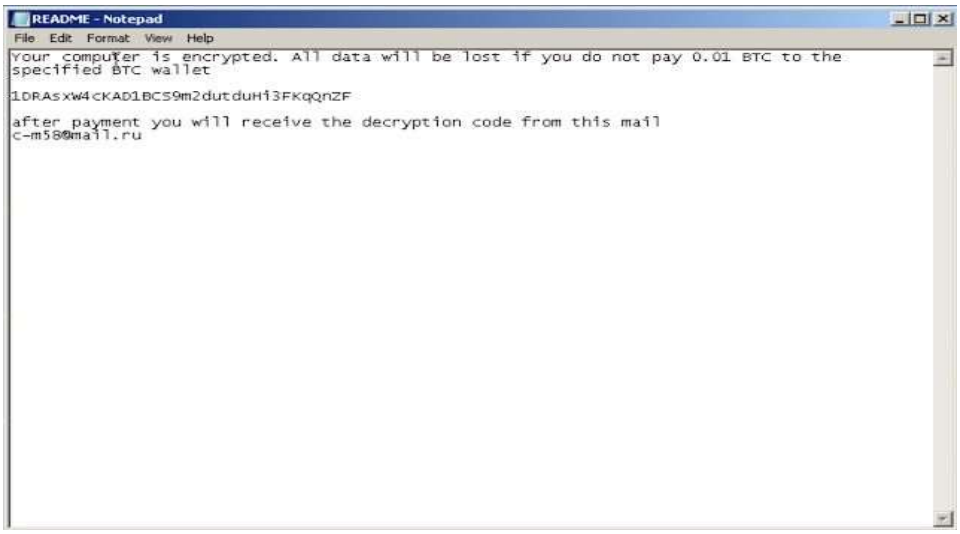


This image depicts a successful decryption session using the Thanatos Decryptor tool. The interface provides real-time verification of decrypted files, including details such as calculated seed values, decrypted file names, and logged results. This confirms the tool's effectiveness in identifying and restoring files encrypted by Thanatos ransomware, generating valuable session logs and validation outputs for forensic analysis.

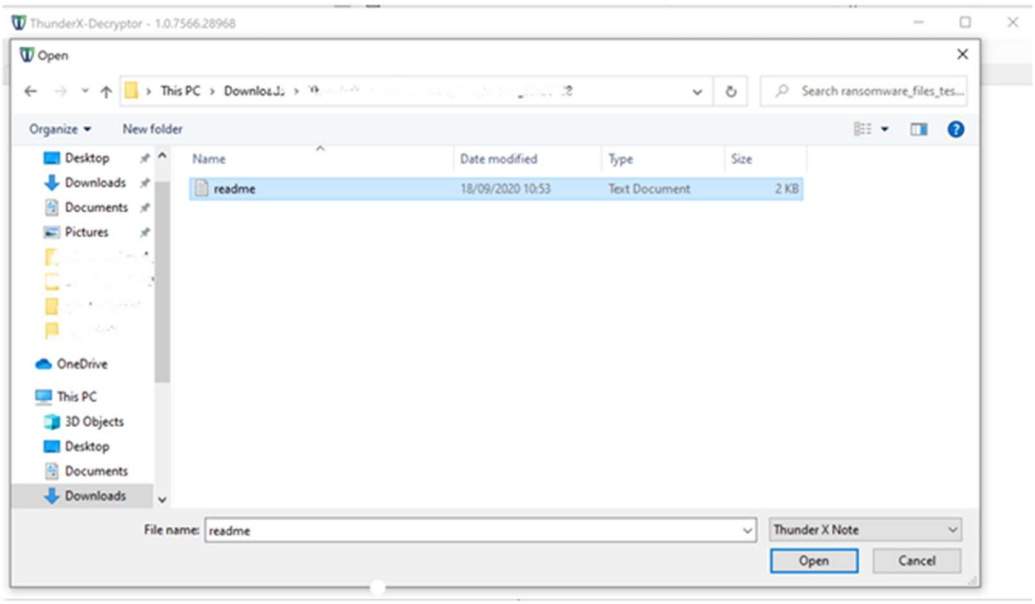
5.2. ThunderX Decryptor Workflow



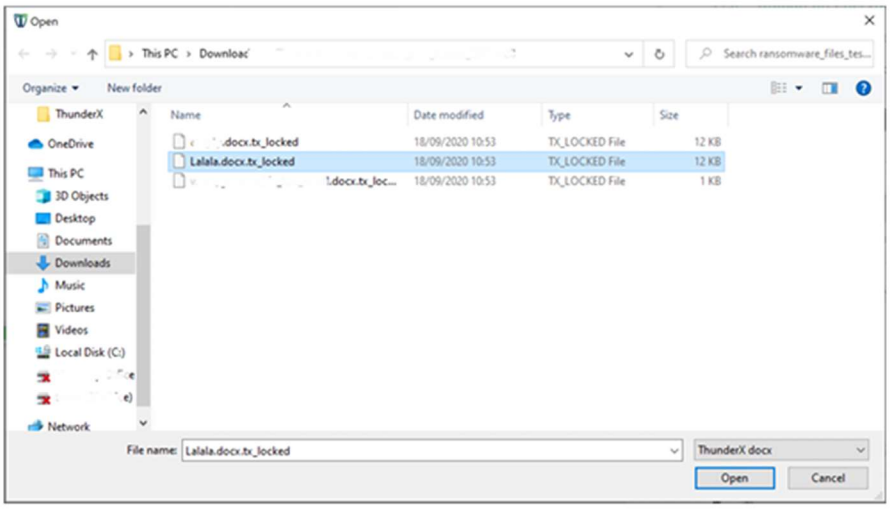
This screenshot shows the ThunderX-Decryptor application instructing the user on its step-by-step file decryption workflow. The interface clearly details how to upload a ransom note, optionally select an encrypted file (supporting formats like `.docx`, `.pptx`, `.xlsx`, or `.zip`), and initiate server-based decryption. It guides users through selecting folders and highlights estimated decryption timing, making the process transparent for forensic analysis and user reporting.



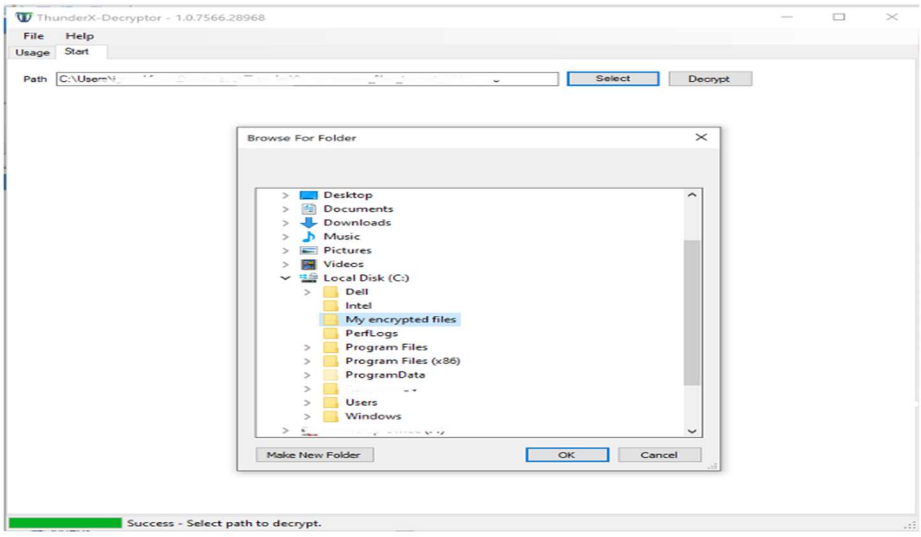
This image displays a typical ransom note file, often named `readme.txt`, which is a critical input for the ThunderX Decryptor. This note provides unique identifiers and encryption details necessary for the tool to analyze the infection and attempt file recovery.



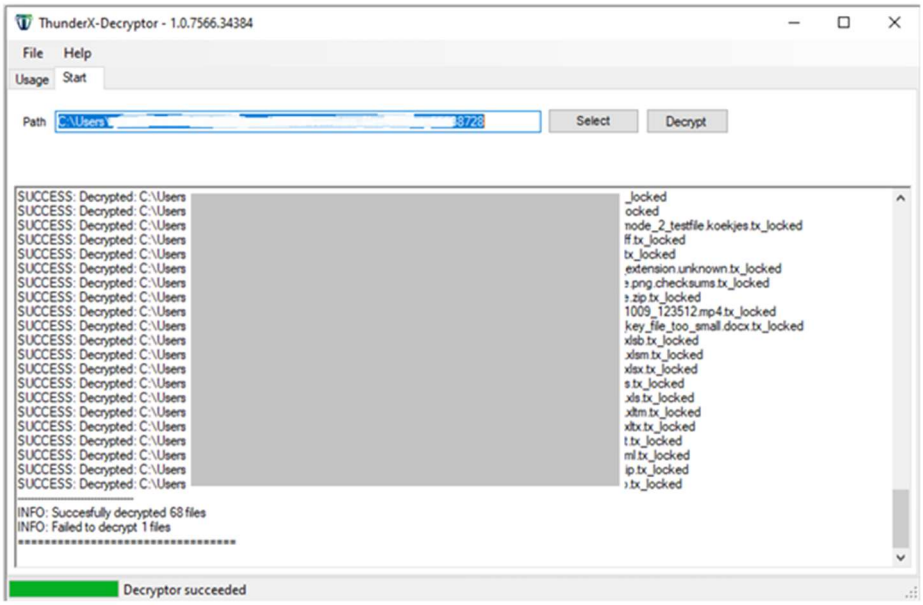
This open file dialog within the ThunderX Decryptor tool prompts the user to select the ransom note file (`readme.txt`), a required step for the decryption process. This is crucial for providing the tool with the necessary information to analyze the ransomware variant and initiate the decryption of files affected by ThunderX, highlighting an essential phase in the incident response workflow.



This standard Windows file selection dialog displays multiple files bearing the `.tx_locked` extension, clearly indicating documents that have been encrypted by ThunderX ransomware. The user is prompted to select an encrypted file for decryption, visually illustrating a crucial step in the ransomware recovery workflow and providing direct evidence of affected files prior to remediation.



This image shows the ThunderX Decryptor's folder browse dialog, which prompts the user to select the directory containing encrypted files for decryption. This interface allows for targeted selection of affected folders, ensuring that the decryption process is applied precisely to locations impacted by ThunderX ransomware. The clarity of this step is vital for precise and efficient remediation during incident response procedures.



This image captures the ThunderX Decryptor's status window displaying a progress bar and the message “Decryption succeeded.”. This visual feedback confirms the successful completion of the file decryption process, indicating that encrypted files in the selected directory have been processed and restored. Such status indications are vital for validating remediation outcomes and documenting steps taken during incident response and ransomware recovery workflows.

6. Summary Table

Summary Point	Details
Recovery Objective	File decryption after Thanatos/ThunderX attack
Operation	Batch/single file, CLI/GUI, session logging
User	IT, DFIR Analyst, System Admin
Key Features	Fast, no ransom, reporting, audit support
Limitation	Not all new strains are covered; success varies by version
Improvements Suggested	Wider variant support; improved GUI; advanced error logs
Good Points	Free, safe, trusted by cybersecurity community

7. 15-Liner PoC Summary

1. Recovers Thanatos/ThunderX ransomware-encrypted files.
2. CLI and GUI versions are available, varying by tool.
3. Supports both batch and single file decryption.
4. Identifies valid ransomware strains before initiating decryption.
5. Reports on both successful and failed decryption attempts.
6. Integrates effectively with digital forensic workflows.

7. Features lightweight and portable deployment.
8. Provides step-by-step operation logs for traceability.
9. Functions post-infection, typically before a full system reimage.
10. Community-updated for compatibility with emerging ransomware versions.
11. Suitable for critical incident response and post-breach recovery scenarios.
12. No cost to deploy as they are open/free tools.
13. Recommended by major cyber defense teams and organizations.
14. Offers clear evidence for legal and audit compliance needs.
15. Does not generally require administrator/root access for basic operation.

8. Time to Use / Scenarios

These tools are best utilized in the following scenarios:

- After a system has been encrypted by Thanatos or ThunderX ransomware and is safely isolated.
- During digital forensic or law enforcement casework to facilitate data recovery.
- To restore critical operations before a full system re-imaging, minimizing business disruption.

9. When to Use During Investigation

In the course of an investigation, these tools are applied:

- Post-infection, specifically after securing and isolating affected devices.
- During the evidence collection phase to demonstrate the feasibility of file recovery.
- To support internal reporting and compliance audits by providing proof of remediation.

10. Best Person to Use & Required Skills

- **Best Users:** Digital Forensics Analysts, IT Security Responders, System Administrators.
- **Skills Needed:**
    - Knowledge of ransomware behaviors and effects.
    - Ability to competently use CLI or GUI tools on Windows platforms.
    - Familiarity with forensic investigation protocols and methodologies.
    - Meticulous evidence documentation practices.

11. Flaws & Suggestions for Improvement

- **Limited Variant Support:** Support for updated ransomware variants/versions can be limited unless community updates are rapid.
- **GUI Enhancement:** The Graphical User Interface could be further enhanced for improved usability by beginners.
- **Decryption Guarantee:** Decryption is not always guaranteed for all encrypted files or ransomware variants.

- **Logging & Reporting:** Expanded error reporting and customizable logging options would greatly benefit compliance and detailed analysis.

12. Good About These Tools

- **Cost-Effective & Safe:** They are free and reputable tools, eliminating the risk of paying a ransom.
- **Efficiency:** They save time and facilitate the recovery of operational data.
- **Transparency:** Provide clear, comprehensive logs for reporting and analysis.
- **Trust & Reliability:** Highly trusted by law enforcement agencies and IT security professionals.

13. References

- NoMoreRansom Project – Thanatos Decryptor
- BleepingComputer Ransomware Decryptors

14. Conclusion

This Proof of Concept (POC) report demonstrates the practical application and effectiveness of the Thanatos Decryption Tool and ThunderX Decryptor in ransomware incident response. By leveraging these tools, organizations can significantly reduce the impact of ransomware attacks by restoring encrypted data without paying ransom demands.

The detailed investigation steps, combined with methodological evidence collection and clear documentation practices, ensure a thorough and transparent incident response process. Continuous tool updates and integration with forensic best practices further strengthen cybersecurity defenses.

It is recommended that organizations incorporate these decryptors into their incident response toolkits and maintain readiness through regular testing in isolated environments.

Prepared by:

Prajwal Sharma

Internship ID: 402

Digisuraksha Parhari Foundation

July 2025