Ransomware Simulation Report

Report Generated on: 2025-03-02 17:19:33

System Information:

OS: Windows

OS Version: 10.0.22631

System Name: HP

Username: leenh

IP Address: 192.168.82.44

Summary

Total Files Encrypted: 13

Total Files Decrypted: 7

Encrypted Files:

Encrypted: ransomware_test\README.txt

Encrypted: ransomware_test\test1.txt.txt

Encrypted: ransomware_test\test2.docx.txt

Encrypted: ransomware_test\README.txt

Encrypted: ransomware_test\test1.txt.txt

Encrypted: ransomware_test\test2.docx.txt

Encrypted: ransomware_test\README.txt

Encrypted: ransomware_test\test1.txt.txt

Encrypted: ransomware_test\test2.docx.txt

Encrypted: ransomware_test\README.txt

Encrypted: ransomware_test\test1.txt

Encrypted: ransomware_test\README.txt

Ransomware Simulation Report

Encrypted: ransomware_test\test1.txt

Decrypted Files:

Decrypted: ransomware_test\test1.txt.txt

Decrypted: ransomware_test\test2.docx.txt

Decrypted: ransomware_test\test1.txt.txt

Decrypted: ransomware_test\test2.docx.txt

Decrypted: ransomware_test\test1.txt.txt

Decrypted: ransomware_test\test1.txt

Decrypted: ransomware_test\test1.txt

Security Analysis & Recommendations:

This simulation demonstrates how ransomware encrypts files.

To protect against real ransomware attacks:

1. Keep systems and software updated.
2. Use endpoint protection and firewalls.
3. Backup critical files regularly.
4. Avoid opening suspicious links or email attachments.
5. Implement strong access controls.

Always test ransomware simulations in a safe environment!