Ransomware Simulation Report

Educational Purpose Only - Run in Isolated VM

Report Information

Field	Value
Date	2026-02-17 21:13:29
User	deadbeat
Computer	WIN10

Simulation Summary

Metric	Value
Files Encrypted	36
Files Decrypted	36
VM Protection	■ Active
Files Restored	■ Yes

Encryption Details

• Algorithm: AES-256 in CBC mode • Key Derivation: PBKDF2 with SHA256 • Salt: educational_salt_2024 • Iterations: 100,000 • File Extension: .encrypted

Learning Outcomes

✓ How ransomware encrypts files ✓ File extension changes (.encrypted) ✓ Ransom note delivery mechanisms ✓ Importance of backups ✓ VM isolation for malware analysis ✓ Encryption/decryption processes ✓ Windows API interactions

Prevention Recommendations

1. 3-2-1 Backup Strategy: - 3 copies of data - 2 different media types - 1 copy offsite/offline 2. Security Best Practices: - Keep software updated - Use modern EDR solutions - Enable ransomware protections - Regular security training 3. System Hardening: - Disable unnecessary features - Restrict write access - Enable Controlled Folder Access - Regular vulnerability scans

Success Indicators

Indicator	Status
Files Encrypted	■ 36 files
Ransom Notes Created	■ Yes
Files Decrypted	■ 36 files
Data Integrity	■ Preserved
VM Snapshot Used	■ Yes

Simulation Timeline

Step	Action	Status
1	Environment Setup	■ Complete
2	Test File Creation	■ Complete
3	Encryption Phase	■ 36 files
4	Ransom Note Delivery	■ Complete
5	Analysis	■ Complete
6	Decryption Phase	■ Complete
7	VM Snapshot Restore	■ Ready

Technical Components

• encryption_handler.py: AES-256 encryption/decryption • file_scanner.py: Target file discovery • windows_api.py: Windows API interactions • ransom_note.py: Ransom note generation • ransomware_sim.py: Main orchestrator • analyze_attack.py: Post-attack analysis