Malware Classification Report

1. Executive Summary

This report classifies and analyzes a malware sample based on static indicators, dynamic behavior, and threat intelligence mapping.

Overall Risk Level: High

Likely Category: Ransomware (Crypto-ransomware)

2. Sample Identification

File Type: Windows Portable Executable (PE)

3. Malware Classification

Primary Category: Ransomware

4. Static Analysis Findings

Suspicious cryptographic and file-handling API usage detected.

5. Dynamic Analysis Findings

File encryption, persistence creation, and outbound network attempts observed.

6. Impact Assessment

Severe impact on confidentiality, integrity, and availability.

7. MITRE ATT&CK; Mapping

T1486 – Data Encrypted for Impact

8. Detection & Mitigation

System isolation, patching, backups, and EDR recommended.

Conclusion

This malware presents a high operational risk and requires immediate remediation.