**Malware Analysis Report: Ransomware Simulation**

**1. Introduction**

The ransomware simulation project simulates the basic behavior of a ransomware attack using file encryption. It demonstrates how ransomware might target files in a system, encrypt them using base64 encoding, and then potentially decrypt the files if the correct key or method is provided.

**2. Malware Behavior**

* **Encryption Process**:
  + The ransomware targets files in a specific directory and encrypts them using a base64 encoding algorithm.
  + The script uses a simple file reader to read the content of files, then it applies base64 encoding, transforming the file data into an unreadable format.
  + Encryption occurs in place, meaning the original files are overwritten with their encrypted versions.
* **Decryption Process**:
  + A separate script is used for decrypting the files by reversing the base64 encoding.
  + This allows the restoration of the original files if the correct decryption function is applied.

**3. File Analysis**

* **Encrypted Files**:
  + Files encrypted by the ransomware have the .enc extension.
  + The content of the encrypted files consists of base64-encoded data, which can be identified by the lack of readable text within the file.
* **Decrypted Files**:
  + After running the decryption script, the files are restored to their original readable format, which can be viewed in a text editor.

**4. System Behavior and Impact**

* **File System Modification**:
  + The ransomware modifies the content of all files in the targeted directory, including those not intended for encryption (excluding encryption.py and decryption.py as specified).
  + The ransomware’s in-place encryption leaves no trace of the original content without proper decryption.
* **Potential for Damage**:
  + While this simulation does not cause permanent harm, in a real ransomware attack, encrypted files may become unrecoverable without a decryption key or method, leading to data loss.

**5. Indicators of Compromise (IoC)**

* **File Extensions**:
  + Files encrypted by the ransomware will have the .enc extension.
* **File Content**:
  + Encrypted files will contain base64-encoded data, which will appear as garbled characters when opened in a text editor.

**6. Detection and Mitigation**

* **Detection**:
  + Monitoring changes in file extensions and observing file content transformations (from readable text to encoded data) can help in identifying ransomware activity.
  + Security tools that flag abnormal file modifications or high CPU usage during encryption processes can also detect ransomware behavior.
* **Mitigation**:
  + Ensure that backups of important files are stored securely and regularly.
  + Implement security measures like endpoint protection, email filtering, and network segmentation to prevent ransomware infections.

**7. Conclusion**

This ransomware simulation demonstrates the basic functionality of file encryption and decryption in a controlled environment. While the simulated malware is harmless, it highlights the essential behavior and impact of ransomware. Further analysis and testing can improve defenses and detection strategies against real-world ransomware attacks.