Ransomware Demo: Quick Guide

1 What This Project Does

This is a demo ransomware project that shows how ransomware works:

- Victim gets infected
- Files get encrypted with AES
- Ransom screen appears
- Attacker holds the key needed to decrypt files

2 Main Components

- **attacker_server.py** - The server run by the "attacker"
- **mainencrypt.py** - The malware that encrypts files on victim's computer
- **gui.py** - Shows the ransom message
- **decrypt_aes_key.py** - How the attacker recovers keys

3 How It Works

1. Victim runs `mainencrypt.py` (gets "infected")
2. Malware connects to attacker server
3. Server sends RSA public key to victim
4. Victim generates random AES key and encrypts files
5. Victim encrypts AES key with RSA public key and sends it to server
6. Ransom GUI appears, asking for payment
7. Attacker can recover AES key using `decrypt_aes_key.py`
8. Victim enters key in GUI to decrypt files

4 How to Run the Demo

4.1 Step 1: Start the attacker server

```
python attacker_server.py
```

This starts listening for victims.

4.2 Step 2: Run the "malware" on victim machine

```
python mainencrypt.py
```

This will:

- Connect to the server
- Encrypt your files
- Show the ransom message

4.3 Step 3: Recover the decryption key (attacker side)

```
python decrypt_aes_key.py
```

This will show the key needed to decrypt files.

4.4 Step 4: Decrypt the files

Enter the key from Step 3 into the ransom GUI and click "Decrypt".

5 Important Tips

- Only run this on test files! It really encrypts them!
- Make sure to start the server before running the malware
- If something breaks, check the code - it's pretty straightforward
- Don't actually use this on anyone's computer without permission

6 What to Look At in the Code

- How the encryption uses both RSA and AES together
- How the communication works between victim and server
- How keys are generated and stored
- How the GUI shows the ransom demand

That's it! This demo shows the basic concept of how ransomware works in a simple way.