This is the super sensitive, confidential document that was affected by the ransomware. Congratulations on the bruteforce!

You can paste your bruteforce script in the box below:

|  |
| --- |
| from zipfile import ZipFile, BadZipFile  # Attempt to extract the zip file using the provided password  def attempt\_extract(zf\_handle, password):      try:          # Password must be in bytes          zf\_handle.extractall(pwd=password.strip())          print("[+] Password found: {}".format(password.decode()))          return True      except RuntimeError:          # Incorrect password          return False      except BadZipFile:          print("[-] Corrupted or invalid ZIP file.")          return True  def main():      print("[+] Beginning bruteforce")      try:          # Open the zip file          with ZipFile('enc.zip') as zf:              with open('rockyou.txt', 'rb') as password\_list:                  for password in password\_list:                      if attempt\_extract(zf, password):                          break                  else:                      print("[-] Password not found in the list.")      except FileNotFoundError as e:          print(f"[!] File not found: {e}")  if \_\_name\_\_ == "\_\_main\_\_":      main() |