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:

|  |
| --- |
| import zipfile  from zipfile import ZipFile  # Attempt to extract the zip file with the given password  def attempt\_extract(zf\_handle, password):  try:  zf\_handle.extractall(pwd=password)  print(f"[+] Password found: {password.decode('utf-8')}")  return True  except (RuntimeError, zipfile.BadZipFile):  # Wrong password  return False  def main():  print("[+] Beginning bruteforce ")  try:  with ZipFile('enc.zip') as zf:  with open('rockyou.txt', 'rb') as f:  for password in f:  password = password.strip() # Remove newline characters  if attempt\_extract(zf, password):  print("[+] Extraction successful")  break  else:  print("[+] Password not found in the list")  except FileNotFoundError as e:  print(f"[-] File not found: {e}")  except Exception as e:  print(f"[-] An error occurred: {e}")  if \_\_name\_\_ == "\_\_main\_\_":  main() |