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 sys  def main(args):  print(“Hello World”)  if \_\_name\_\_ == “\_\_main\_\_”:  main(sys.argv)  '''  Forage AIG Cybersecurity Program  Bruteforce starter template  '''  from zipfile import ZipFile  def attempt\_extract(zf\_handle, password):  try:  zf\_handle.extractall(pwd=password.encode('utf-8'))  return True  except Exception as e:  return False  def main():  print("[+] Beginning brute force attack")  with ZipFile('enc.zip') as zf:  with open('rockyou.txt', 'r', encoding='utf-8', errors='ignore') as f:  for line in f:  password = line.strip() # Remove any leading/trailing whitespace  print(f"[-] Trying password: {password}")  if attempt\_extract(zf, password):  print(f"[+] Success! Password found: {password}")  return  print("[-] Password not found in list")  if \_\_name\_\_ == "\_\_main\_\_":  main() |