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())          return True      except:          return False  def main():      print("[+] Beginning bruteforce ")      with ZipFile('enc.zip') as zf:          with open('rockyou.txt', 'rb') as f:              # Iterate through password entries in rockyou.txt              for line in f:                  password = line.strip().decode()                  print(f"[\*] Trying password: {password}")                  # Attempt to extract the zip file using each password                  if attempt\_extract(zf, password):                      print(f"[+] Password found: {password}")                      return      print("[+] Password not found in list")  if \_\_name\_\_ == "\_\_main\_\_":      main()  '''  The script defines a function attempt\_extract() that attempts to extract the encrypted zip file with a given password.   The function returns True if the password is correct and the file can be extracted, and False otherwise.  The main() function reads the encrypted zip file using the ZipFile() method and reads the password list from the rockyou.txt file.  It then iterates through each password in the list and attempts to extract the zip file using the attempt\_extract() function.  If the correct password is found, the script prints the password and terminates. If the correct password is not found,   the script prints a message indicating that the password was not found in the list.  Note: This script is for educational purposes only and should not be used for any illegal or unethical activities.  ''' |