**Bad Ransomware!**

This challenge is based on real ransomware.

**Text:**

A cookie factory was attacked by the “Bad Ransomware!” ransomware gang. All their cookie recipes have been encrypted.

It is your job to recover the cookie recipes!

You have one advantage: you know that the cryptographic design of their ransomware application is flawed.

Good luck!

**Difficulty: high**

Filename: cookies.zip.Encrypted

SHA-256 a95840374aa2f10898eeb9a36f97a760df6d124484d0454e7172b80eeccc321f

**Solution:**

This ransomware (a real sample) partially encrypts the ransomed files (for performance reasons). Each file is divided in 10 blocks, and that start of each block is encrypted, not the rest.

The metadata added by the ransomware application (after magic sequence RANSOMWARE\_METADATA) defines which part of the file have been encrypted: POSITION1:SIZE#POSITION2:SIZE#...

Encryption is done with XOR using a 16-byte long key: the first 16 bytes of a block are encrypted with that key, then the next 16 bytes of that same block are encrypted with the same key, and so on, until the first 256 bytes of each block are encrypted.

The encrypted file is a ZIP file. ZIP files contain redundant information: each file stored inside a ZIP container has 2 records: a ZIPFILE record and a ZIPDIRRECORD. Each type of record contains information like the filename, file timestamps, ... A ZIP file is build up of a series of ZIPFILE records, each followed by the compressed file content. There is one ZIPFILE record per file. After all ZIPFILE records plus compressed data have been stored inside the ZIPFILE, the ZIPDIR records are appended. There is also one ZIPDIR record per file. And finally, a END OF DIRECTORY record is appended.

Because the ransomed file is partially encrypted, the first ZIPFILE record is encrypted, but the corresponding ZIPDIR record is not. With the redundant information in the ZIPDIR record, the first 16 bytes of the ZIPFILE record can be reconstructed, and thus the 16-byt XOR key can be recovered (by XORing the ciphertext with the cleantext).

NVISO has handled a case with ransomware just like this. The only thing that was changed in the metadata, is the magic sequence: this was not RANSOMWARE\_METADATA.

**FLAG:**

CSC{HD6E8HDKZNDKE090AJ}

**Scripts:**

connemara-extract-keystream.py -z -w keystream.bin cookies.zip.Encrypted

connemara-decryptor.py -k keystream.bin cookies.zip.Encrypted