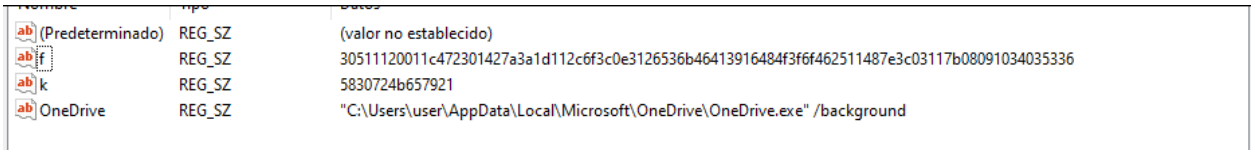
El binario escribe en el registro de windows 2 valores en hexadecimal:

- F = la flag cifrada con una llave XOR
- K = la llave XOR



(Predeterminado)	REG_SZ	(valor no establecido)
f	REG_SZ	30511120011c472301427a3a1d112c6f3c0e3126536b46413916484f3f6f462511487e3c03117b08091034035336
k	REG_SZ	5830724b657921
OneDrive	REG_SZ	"C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

Estos valores vienen en los recursos embebidos del binario

Con esto el participante solo tiene que hacer el algoritmo para descifrar los bytes de la flag

Sin embargo el camino para llegar a esa función tiene código espagueti, código que no funciona y codigo dummy

Tenemos el solver

Python

```python
key = "X0rKey!".encode("ascii")
final2 =
bytes.fromhex("30511120011c472301427a3a1d112c6f3c0e3126536b464139164
84f3f6f462511487e3c03117b08091034035336").decode("ascii")
decode = ""
x = 0
print(final2)
for f in final2.encode("ascii"):
    # print(key[x], f)
    decode += chr(key[x] ^ f)
    # print(chr(key[x]))
    x += 1
    if x == 7:
        x = 0
print(decode)
```

Con esto tenemos de manera muy sencilla un reto 101 de reversing .NET