¡No abras ese PDF!

Al recibir el archivo PDF, toca evitar su ejecución directa. Para ello utilicé la herramienta pdf-parser.py, que permite inspeccionar la estructura interna del PDF y detectar objetos sospechosos sin abrir el archivo.

La pueden descargar con el comando:

wget https://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/pdf-parser.py

Durante el análisis del PDF se identifica un objeto de tipo /Action con la directiva /S /JavaScript, lo que indicaba la presencia de código JavaScript embebido que se ejecutaría al abrir el documento. Al extraer dicho objeto en formato raw, se obtiene el código JavaScript completo incrustado en el PDF.

Al revisar el código JavaScript extraído, se observa que contenía una cadena codificada en **Base64** y una clave definida directamente dentro del script. Además, el código implementaba una función que aplicaba una operación **XOR** byte a byte entre los datos decodificados y la clave, repitiéndola a lo largo de todo el contenido. El resultado de esta operación era mostrado mediante una alerta al abrir el PDF.

Para evitar ejecutar el JavaScript directamente desde el PDF, se debe replicar la lógica de descifrado en un script de Python. En este script se decodifica la cadena Base64 para obtener los datos cifrados y luego aplica la misma operación XOR utilizando la clave identificada en el código JavaScript.

```
import base64

cipher_b64 = "EyUnCTEXIzw4UCsoFwBRYlwrAlViCx4="
key = "UltraSecretKey!"

cipher = base64.b64decode(cipher_b64)

out = ""
for i in range(len(cipher)):
out += chr(cipher[i] ^ ord(key[i % len(key)]))

print("FLAG DECODIFICADA:", out)
```