

WriteUP Reverse 200. KrasCTF 2017

Программа достает из изображения массив данных длиной 12 элементов.

```
CMP DWORD PTR SS:[EBP-8],7
JG SHORT 200.00401550
MOV DWORD PTR SS:[EBP-C],0
CMP DWORD PTR SS:[EBP-C],0B
JG SHORT 200.00401549
MOV BYTE PTR SS:[EBP-2],1
MOV EAX,DWORD PTR SS:[EBP+8]
MOV DWORD PTR SS:[ESP+C],EAX
MOV DWORD PTR SS:[ESP+8],1
MOV DWORD PTR SS:[ESP+4],1
LEA EAX,DWORD PTR SS:[EBP-1]
MOV DWORD PTR SS:[ESP],EAX
CALL <JMP.&msvcrt.fread>
MOUZX EDX,BYTE PTR SS:[EBP-1]
LEA EAX,DWORD PTR SS:[EBP-2]
AND BYTE PTR DS:[EAX],DL
MOUSX EAX,BYTE PTR SS:[EBP-2]
MOV ECX,DWORD PTR SS:[EBP-8]
SHL EAX,CL
MOV BYTE PTR SS:[EBP-2],AL
MOV EAX,DWORD PTR SS:[EBP+C]
MOV ECX,DWORD PTR SS:[EBP-C]
ADD ECX,EAX
MOV EAX,DWORD PTR SS:[EBP+C]
MOV EDX,DWORD PTR SS:[EBP-C]
ADD EDX,EAX
MOUZX EAX,BYTE PTR SS:[EBP-2]
ADD AL,BYTE PTR DS:[EDX]
MOV BYTE PTR DS:[ECX],AL
LEA EAX,DWORD PTR SS:[EBP-C]
INC DWORD PTR DS:[EAX]
JMP SHORT 200.004014E9
LEA EAX,DWORD PTR SS:[EBP-8]
INC DWORD PTR DS:[EAX]
JMP SHORT 200.004014DC
```

Но при расшифровке сообщения используются 11 элементов.

```
CMP DWORD PTR SS:[EBP-140], 0A
JG SHORT 200.0040146D
LEA EAX, DWORD PTR SS:[EBP-8]
ADD EAX, DWORD PTR SS:[EBP-140]
SUB EAX, 130
MOVZX EDX, BYTE PTR DS:[EAX]
LEA EAX, DWORD PTR SS:[EBP-11B]
XOR BYTE PTR DS:[EAX], DL
LEA EAX, DWORD PTR SS:[EBP-8]
ADD EAX, DWORD PTR SS:[EBP-140]
SUB EAX, 120
MOVZX EAX, BYTE PTR DS:[EAX]
AND AL, BYTE PTR SS:[EBP-11B]
MOV BYTE PTR SS:[EBP-139], AL
MOVSX EAX, BYTE PTR SS:[EBP-139]
MOV DWORD PTR SS:[ESP], EAX
CALL <JMP.&msvcrt.putchar>
LEA EAX, DWORD PTR SS:[EBP-140]
INC DWORD PTR DS:[EAX]
JMP SHORT 200.00401415
MOV DWORD PTR SS:[ESP], 200.00403059
```

Двенадцатый элемент необходим именно для расшифровки, но вместо него используется значение, лежащее по адресу 0060FE1D.

| | | |
|----------|----------|-------|
| 0060FE10 | F0F9FFFF | яяшр |
| 0060FE14 | EFE6DFF4 | фЯжп |
| 0060FE18 | 24E5E3F2 | тге\$ |
| 0060FE1C | 00000004 | ... |
| 0060FE20 | 79706170 | рару |
| 0060FE24 | 2E737572 | rus. |

Поэтому патчим цикл расшифровки и получаем флаг.

```

[00401460]
[00401460] CMP DWORD PTR SS:[EBP-140],0A
[00401461] JG SHORT 200.0040146D
[00401462] LEA EAX,DWORD PTR SS:[EBP-8]
[00401463] ADD EAX,DWORD PTR SS:[EBP-140]
[00401464] SUB EAX,130
[00401465] MOVZX EDX,BYTE PTR DS:[EAX]
[00401466] LEA EAX,DWORD PTR SS:[EBP-11D]
[00401467] XOR BYTE PTR DS:[EAX],DL
[00401468] LEA EAX,DWORD PTR SS:[EBP-8]
[00401469] ADD EAX,DWORD PTR SS:[EBP-140]
[0040146A] SUB EAX,120
[0040146B] MOVZX EAX,BYTE PTR DS:[EAX]
[0040146C] AND AL,BYTE PTR SS:[EBP-11D]
[0040146D] MOV BYTE PTR SS:[EBP-139],AL
[0040146E] MOVSX EAX,BYTE PTR SS:[EBP-139]
[0040146F] MOV DWORD PTR SS:[ESP],EAX
[00401470] CALL <JMP.&msvcrt.putchar>
[00401471] LEA EAX,DWORD PTR SS:[EBP-140]
[00401472] INC DWORD PTR DS:[EAX]
[00401473] JMP SHORT 200.00401415
[00401474] MOV DWORD PTR SS:[ESP],200.00403059
```

Hello! Give me file for translation: papyrus.bmp

Translated text: egypt_force

Для продолжения нажмите любую клавишу . . .