furiousfast.exe

Hash Values:

Using HashMyFiles,

MD5 : 5ce1013a5bc6a894ecf5051dd07f92cd

SHA1: b14dc27783aa760be4aa2ac3ec282a7b070efe05

SHA256: 9c2306783dc9d8f44e36c7725babfeceec03be7bac8d12be93be02925a270d07

File Type:

Using Detect it Easy,

PE32, compiled using FASM

Due to the file being a PE32, IDA can be used to disassemble and debug the program.

Disassembly:

After disassembling the file in IDA, we see that the program intends to make a connection with www.netfixed.com.

```
call    ds:InternetOpenA
push    offset aWwwNetfixedCom ; "www.netfixed.com"
pop     ebx
xor     edi, edi
push    edi             ; dwContext
push    edi             ; dwFlags
push    3               ; dwService
push    edi             ; lpszPassword
```

After double-clicking the offset value of the website, we are navigated to the .data of the program where the flag can be found.

```
data:0040104F                   db 0Dh,0
data:00401051 aF7AndF8Ar3Grea   db 'F7_AND_F8_AR3_GREAT_MOVIES_X-Force',0
data:00401074 ; char Format[3]
data:00401074 Format            db '%s',0               ; DATA XREF: start+5↓o
data:00401077 aWwwNetfixedCom   db 'www.netfixed.com',0 ; DATA XREF: start+1F↓o
data:00401088 aDummymovieMp4    db '/dummymovie.mp4',0  ; DATA XREF: start+3A↓o
data:00401098 ; CHAR szVerb[]
data:00401098 szVerb            db 'GET',0              ; DATA XREF: start+4C↓o
data:0040109C                   align 1000h
data:0040109C  data             ends
```

Flag : F7_AND_F8_AR3_GREAT_MOVIES_X-Force