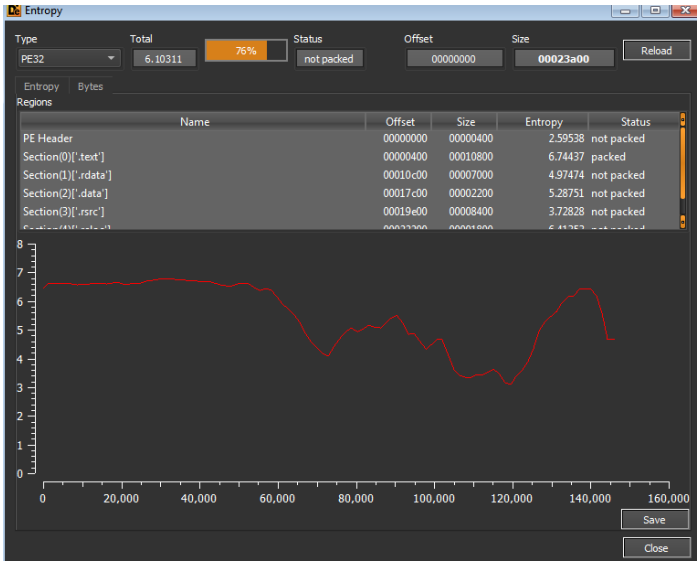
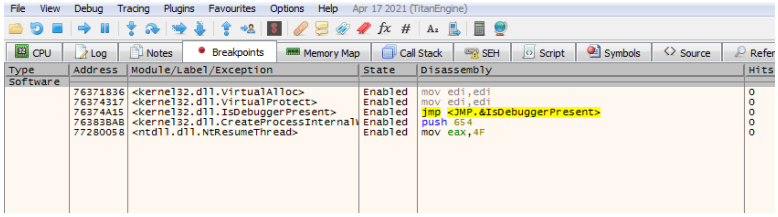
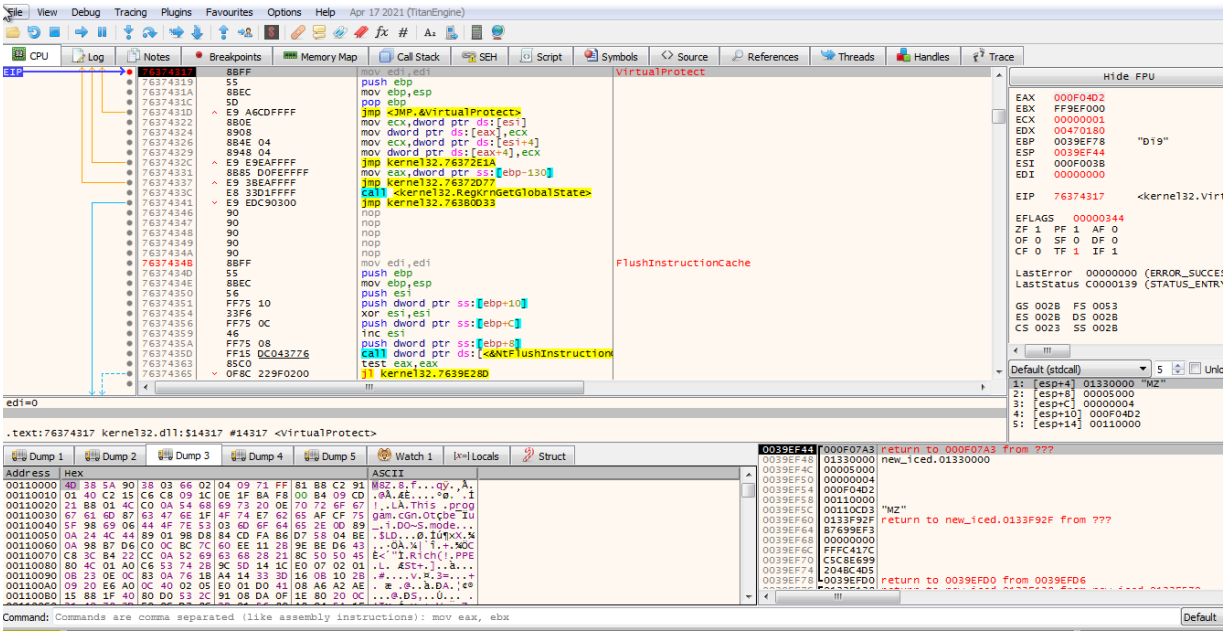
Initially we load the sample in DetectItEasy and here we can note that entropy is fairly high so sample might be packed.



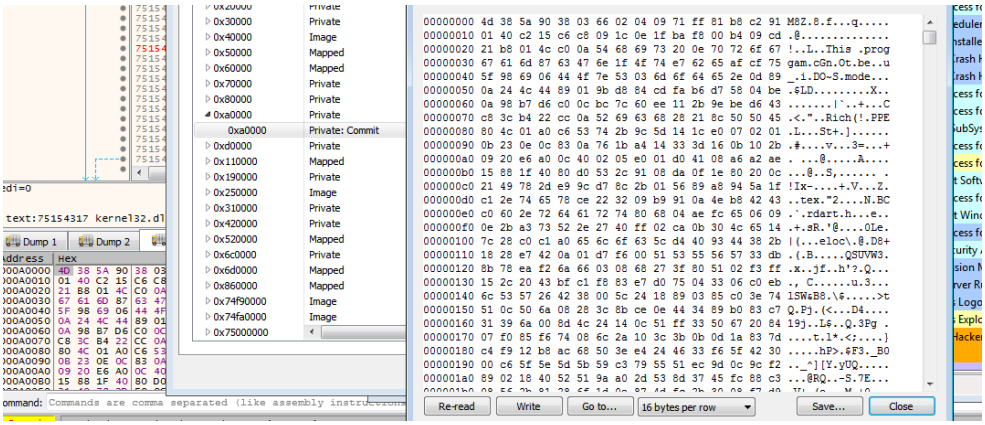
Now we upload the sample in x32 dbg and apply breapoints on VirtualAlloc,VirtualProtect,IsDebuggerPresent,CreateProcessInternalW,NtResumeThread for unpacking.



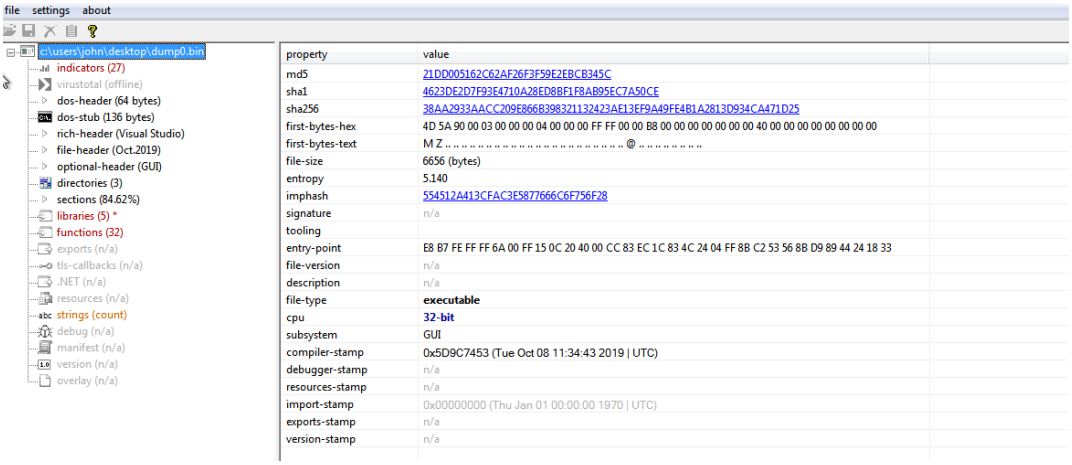
After hitting VirtualAlloc third time we analyse the memory return by it dump3 and we can note that it is containing a PE file compressed with aplib (M8Z), so here we will use aplib-ripper to extract pe.



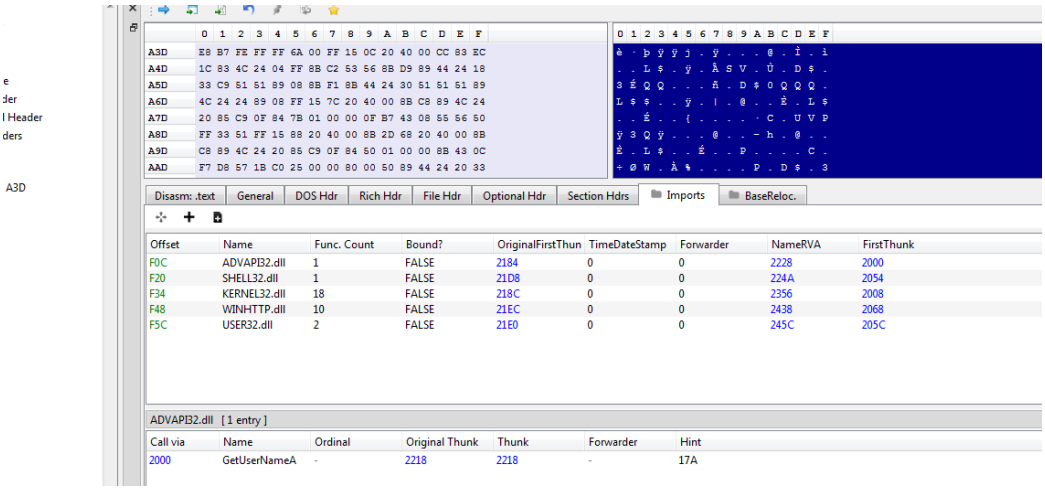
Here we dump the comperssed pe using process hacker and decompress it.



Now we loaded the decompressed pe in pestudio.



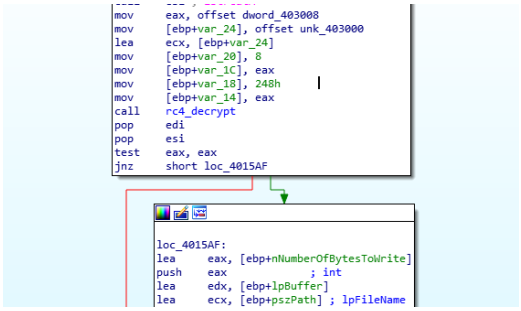
Here as sample is not mapped in memory we can view all the imports are intacted .



Here we can note suspicious APIs it might be trying to make network communication to C2 server.

HeapReAlloc	-	-	kernel32.dll
wsprintfA	-	-	user32.dll
wsprintfW	-	-	user32.dll
WriteFile	x	-	kernel32.dll
VirtualProtect	x	-	kernel32.dll
WinHttpCloseHandle	x	-	winhttp.dll
WinHttpSetOption	x	-	winhttp.dll
WinHttpOpenRequest	x	-	winhttp.dll
WinHttpSendRequest	x	-	winhttp.dll
WinHttpQueryHeaders	x	-	winhttp.dll
WinHttpOpen	x	-	winhttp.dll
WinHttpReceiveResponse	x	-	winhttp.dll
WinHttpQueryDataAvailable	x	-	winhttp.dll
WinHttpConnect	x	-	winhttp.dll
WinHttpReadData	x	-	winhttp.dll

In IDA we can note that arguments to rc4_decrypt are passed and one argument is pointing to location 403000 and another two are pointing to the location 403008 so, 403000 can contain key of rc4_crypt.




```python
from arc4 import ARC4
import pefile

def config_extract(file):
    pe=pefile.PE(file)
    for section in pe.sections:
        if b".data" in section.Name:
            return section.get_data()

def rc4_decrypt(key,data):
    cipher=ARC4(key)
    decrypt=cipher.decrypt(data)
    return decrypt.replace(b'\x00',b'')

def main():
    file=input("file: ")
    data=config_extract(file)
    key=data[:8]
    data=data[8:592]
    print(rc4_decrypt(key,data))

if __name__=="__main__":
    main()
```

```
b'\xfb3=\x1e\x02/index.php\x13boldidiotruss.xyz\x0fnizaoplov.xyz\x0f153ishak.best\x10ilu21plane.xyz'
```