

Forum: [Hack Forums](#)

Thread: [Trying to run unpacked/dumped game executable, but Windows is being a b*tch](#)

SIM-5156932 - February 18, 2022, 8:30 am

I'm trying to reverse engineer the MicroVolts SURGE client so I can try to make a server emulator. Problem is, the main executable is protected with Themida 2 (32-bit), which makes it crazy difficult to unpack. I managed to find two different tools that can dump the unpacked process from memory and reconstruct the IAT, but I can't execute either dumps.

First dump made with pe-sieve contains a seemingly complete IAT, and IDA static analysis seems to have found all the game's code, but when I try to run the executable, I get a "Microsoft Visual C++ Runtime" error (R6034) followed by an application error 0xC0000142.

The second dump was made with Process-Dump (by glmcdona on github), and again, complete IAT, successful IDA analysis, but as soon as I try to execute it, it crashes with a 0xC0000005 access violation error. If I try to debug it in IDA, the exception is thrown before the first instruction in 'start' is reached. This dump seems more promising than the first one, because it loads all the dependent dlls in memory before it crashes, whereas the other dumped exe doesn't even do anything.

I'm not looking for someone to unpack and fix this file for me, I just want some advice/help on what to do next in order to finally make this exe runnable without any errors.

Nevertheless, I've still uploaded the files in case someone want to take a look:
mega.nz/file/ppJwibaS#sacX9bQ5DpRkvOWwyvMf60RIPKfSFLbvwV1qadh8r8s

MicroVolts.exe - original, packed (Themida 2)

400000.MicroVolts.exe - Unpacked with pe-sieve (error 0xC0000142)

MicroVolts_exe_PID980c_MicroVolts.exe_400000_x86.exe - Unpacked with Process-Dump (error 0xC0000005 when run)

sneezing panda - February 19, 2022, 2:25 pm

Gonna be straight up, I have no idea how to do this buuuut.... Have you tried LCF-AT's Olly script?

<https://forum.tuts4you.com/topic/32632-themida-winlicense-manually-unpack-tutorial-exsample/>