Malware Obfuscation

New Attempt

- Due No Due Date
- Points 2
- Submitting a text entry box or a file upload

Imagine you've created a malware named **Eicar**, which is available for download at **Download Anti Malware Testfile - EICAR (https://www.eicar.org/download-anti-malware-testfile/)** (rest assured, it's not harmful!). However, your adversaries, the antivirus companies, have discovered it and created a signature to detect it.

To help your malware evade detection and spread unhindered, you plan to implement an obfuscation technique. Here's what you'll do:

1. Disassemble the Eicar file using NASM (**https://www.nasm.us/pub/nasm/releasebuilds/2.16rc12/ (https://www.nasm.us/pub/nasm/releasebuilds/2.16rc12/)**)
2. Introduce "Dead Code" into the original assembly code.
3. Re-assemble the modified file using NASM or a compatible assembler.

To test your obfuscation's effectiveness, follow these steps:

1. Upload the original Eicar file to VirusTotal (**https://www.virustotal.com/ (https://www.virustotal.com/gui/home/upload)**).
2. Upload your modified version of Eicar to VirusTotal.
3. Compare the results of both scans.

Please provide the following items for submission:

1. The disassembled (original) code of the malware (text format is sufficient; no need to submit files).
2. The modified code of your Eicar malware version (text format is sufficient; no need to submit files).
3. A report where you explain the results you obtained, whether positive or negative.

Will your malware be able to avoid detection? How many antivirus engines have you been able to defeat? Let me know.

NOTES:

- Eicar is **NOT** a real malware!
- Keep in mind, though, that your antivirus will consider Eicar AS a real malware. Anyway, don't worry, it's just a fake malware to test your antivirus software. Trust me. Really.
- You surely do, but if you still don't trust me, visit this wikipedia page: **EICAR test file - Wikipedia (https://en.wikipedia.org/wiki/EICAR_test_file)**
- If the assembler is struggling trying to reassemble your file, try to make the code compatible with it (sometime, the disassembler adds information not understandable to a different assembler)