**Capture the flag exercise: Dynamic Analysis**

* What is the MD5 hash of the file?

**56213d836485ad7afa5ef262085c4a2e**

* What is the SHA256 hash of the file? (Hint: use hash calculator tool)

**3e1d415ec17716efd58d98caa618648f8f3276b230f6ea193378a4e79845e317**

* What file does this program drop? (Hint: use tools like regshot or procmon)

**Part3.txt**

* What registry entry did the program create? (Hint: use tools like regshot or procmon)

**HKU\S-1-5-21-1741230252-4240309174-2391224119-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\xfti\Part2: "V3R53\_3N"**

* What is the mutex name was created to prevent the program from having multiple instances? (Hint: use tools like procmon)

**\Sessions\1\BaseNamedObjects\Part1\_DYN4M1C\_R3**

* To where does this program externally connect? (Hint: use tools like FakeNet-NG, Wireshark, BurpSuite)

**Yes**

* What is the flag? (Hint: The flag was divided in 4 parts)

**DYN4M1C\_R3V3R53\_3NG1N33R\_X-Force**

Part1\_DYN4M1C\_R3

Part2: "V3R53\_3N"

Part3: G1N33

DYN4M1C\_R3 V3R53\_3N G1N33