Drew Hamilton

3/05/19

Most Common 15 Instructions

Out of a total 5479608 instructions, I found that the most common were the following, with the amount I found following, and what the instruction does based upon the intel instruction reference:

mov: 1772921 -> “Load and store control registers”, or it can “Load and store debug registers”

call: 437650 -> Pushes important registers onto the stack and then calls the specified procedure

lea: 337505 -> Loads an address into a register, extraordinarily efficient for certain math purposes

test: 303075 -> gives no output but sets

jmp: 274277 -> The reference says it best: “The TEST instruction performs a logical AND of two operands and sets the SF, ZF, and PF flags according to the results.”

je: 271792 -> “Jump if equal/Jump if zero”

cmp: 259222 -> “The CMP (compare) instruction computes the difference between two integer operands and updates the OF, SF, ZF, AF, PF, and CF flags according to the result”

xor: 223107 -> This instruction simply computes the bitwise XOR operation; The resultant bit is only 1 if the operands are different

nop: 215360 -> quite simply “increments the EIP register to point at the next instruction”

push: 186845 -> pushes an item onto the stack

pop: 183450 -> pops (removes) an item off the stack

jne: 176733 -> jumps if the zero flag is on

add: 146797 -> adds two operators and puts the result into the destination operator

sub: 94446 -> subtracts the second argument from the first and puts it in the location of the first

ret: 61547 -> pops off the stack the important variables pushed on by the CALL instruction. This means that the code returns to the previous task because the EIP register is popped off the stack as well.