תרגיל מחקר לגילוי OPCODE

מיכאל ספקטור יא3

מטרתנו הינה למצוא את ה Opcode של mov ax, dx.

בכדי למצוא אותו קודם כל נעזרתי ברצף פקודות פשוט, שיחקתי קצת עם הפקודות בכדי לנסות להבין האם ישנה חוקיות מסוימת. ניסיתי להריץ אותן הפוך זו לזו וגיליתי שהOpcode של הפקודות כאשר הרגיסטרים הפוכים הינו שונה, דוגמה:

mov ax, bx ;8BC3

mov bx, ax ;8BD8

זה גרם לי לחשוב, איך? למה זה ככה? המשכתי לשחק עם כל מיני רגיסטרים, אך הפעם במקום לדרוס אותם עם ערכים מרגיסטרים אחרים, התחלתי להציב מספרים כגון 2567h.

פקודות לדוגמה:

mov ax, 2567h ;B86725

mov bx, 2567h ;BB6725

כאן שמתי לב לדבר מאוד חשוב: ה B8 התהפך ל 8B כאשר הכנסנו מספרים במקום רגיסטרים לרגיסטרים, מכאן ומבדיקות נוספות הסקתי שה OPCODE מורכב משני בייטים.

ומכאן גם הסקתי שכל פעם שמכניסים רגיסטר לרגיסטר, החלק הראשון של הקוד יהיה B8:

**8 B \_ \_**

כעט נותר לנו למצוא עוד בייט אחד ולמלא את החלק החסר.

בכדי לבצא את השלב האחרון התסבכתי מאוד בהתחלה, מכיוון שלא ידעתי איך אני אמור לעשות זאת. לשם כך חשבתי: "איך אוכל לראות או לזהות שינויים אשר קוראים בחוקיות מסוימת?". לשם כך רשמתי מספר שורות קוד אשר יעזרו לי לזהות זאת:

mov ax, ax ;8BC0

mov ax, bx ;8BC3

mov ax, cx ;8BC1

mov dx, dx ;8BD2

)ערכתי בדיקות נוספות)

לאחר רצף זה, ראיתי בבירור את החוקיות!

כאשר הרגיסטר הימני שאותו אנו דוחסים הינו ax אז ערכו ההקסה דסימלי בOPCODE הינו כלשהו (C0 במקרה שלנו).

כאשר הרגיסטר הימני הינו bx אז ערכו ההקסה דסימלי בOPCODE הינו ערכו של

של ax עם הוספה של +3.

כאשר הרגיסטר הימני הינו cx אז ערכו ההקסה דסימלי בOPCODE הינו ערכו של

של ax עם הוספה של +1.

כאשר הרגיסטר הימני הינו dx אז ערכו ההקסה דסימלי בOPCODE הינו ערכו של

של ax עם הוספה של +2.

מכאן, נוכל לפענח זאת. הopcode של:

mov ax, ax ;8BC0

נעבוד על פי הכלל שקבענו. מה שעלינו למצוא זה mov ax, dx ולכן נוסיף 2+ ונקבל:

**8 B C 2**