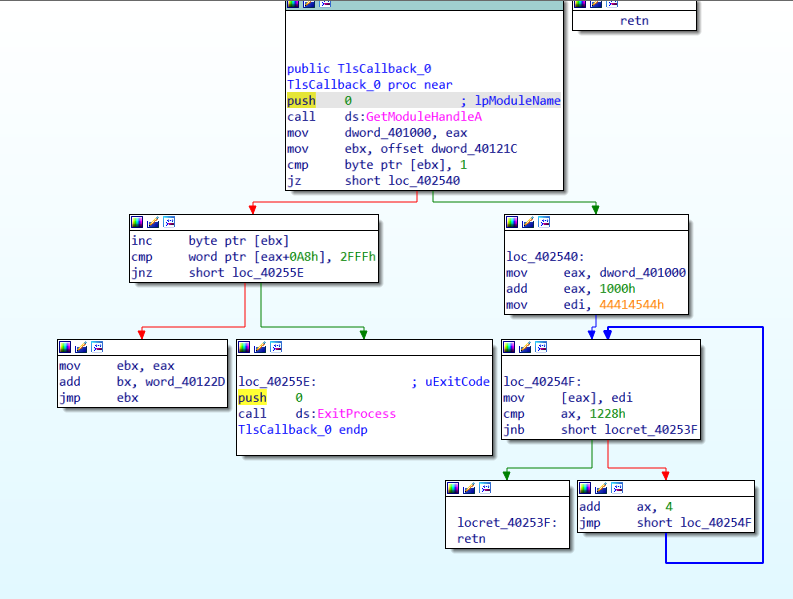
Write Up Anti Debug

1)

את התרגיל אני אנתח עם X32 וIDA

תמונה שמכילה טקסט

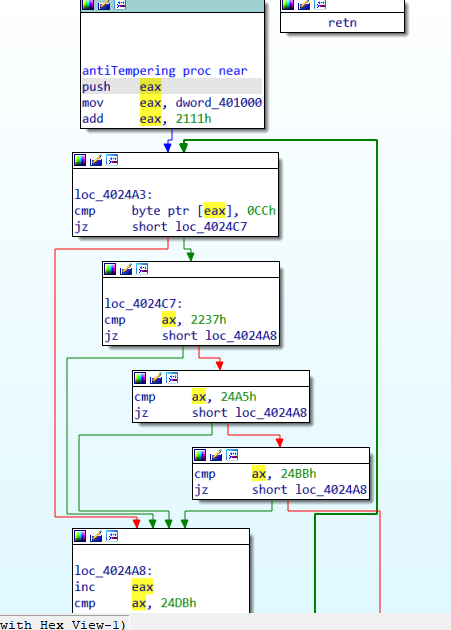
התיאור נוצר באופן אוטומטי יש לנו מספר קטן מאוד של פונקציות, אפשר ככה לנתח כל אחת ולראות מה מעניין אותנו:



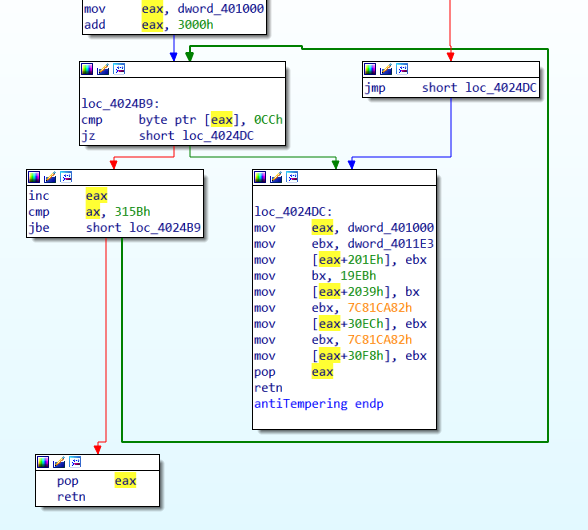


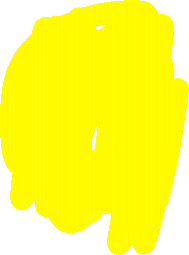
זה הTLS אין כאן קוד זדוני שרוצה לבדוק שאנחנו לא מדבגים אותו אבל יש קפיצה לקוד מצד שמאל

הפונקציה המעניינת הבאה:

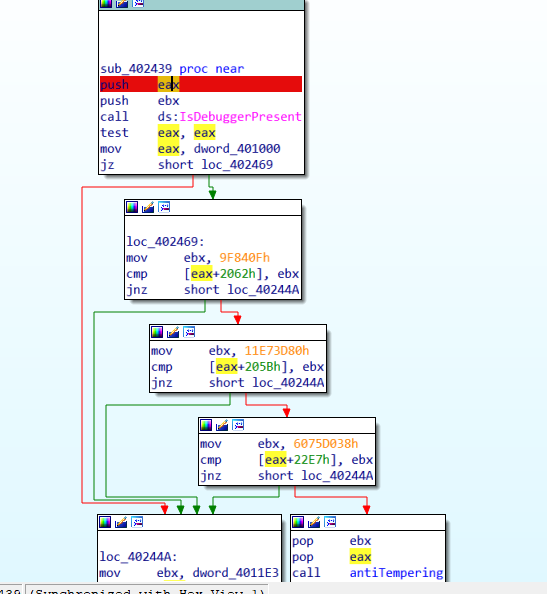


כאן אפשר לראות שיש בדיקה שלא שינינו את הקוד של הפונקציה שלנו במקומות אסטרטגיים.





במקרה שכן שינינו את הקוד התוכנית תלך לאזור המודגש ושם היא תשנה את הקןד באזור מסוים(על פי ההרצה בהמשך זה כדי לצאת מהתהליך)



כאן יש לנו את הבדיקה הראשית אם הדיבאגר פעיל, שאפשר לעבוד על זה בעזרת שינוי של הביט.

ואחר כך יש בדיקה של שורות קוד שלא שינינו ואם כן אנחנו נצטרך לעזוב.

כל מנגנון בעיקרון אפשר לשנות בפני עצמו, למשל את הבדיקה אם הדיבאגר פעיל אפשר לדרוס בפני עצמו. או את הבדיקה של הבתים אפשר להמשיך הלאה בלי לבדוק את התנאי או לא לשנות את התוכנית אם זיהינו שאנחנו מדובאגים ע"י תהליך זר.

2) אני בחרתי דווקא לדרוס את הקריאות שיש לפונקציה של הבדיקה. בשביל לעשות את זה פתחתי בשלב הזה את ה32X וראיתי שיש קריאות לפני תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי הקוד המרכזי לפונקציה של הבדיקה, אך אבוי! הפונקציה שנקראת ראשונה היא הזאת שבודקת האם אני בכלל בתהליך דיבוג, ואכן מה שקורה אחרי שאני מריץ אותה זה:

תמונה שמכילה טקסט

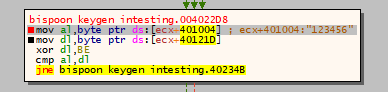
התיאור נוצר באופן אוטומטיוהתוכנית שלנו תצא מיד אחרי הקריאה לפונקציה הזאת, כמובן שאנחנו לא רוצים לצאת מיד ולכן אני דרסתי את הקריאה לפונקציה(גם כי לא היה אף קטע קריטי שיש לבצע בפונקציה.)

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

ככה עשיתי לשאר הקריאות שיש(עוד איזה 2-3 פעמים)

איך גיליתי את הסיסמה:

 זיהיתי שעושים פה השוואה בין מה שיוצא מהקוד הקודם לסיסמה שמכניסים

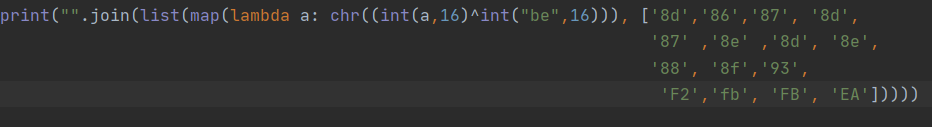




למעשה אנחנו משווים בין 2 המחרוזות האלה

רק שאנחנו עושים קסור של BE עם ההאש שיוצא בלמטה

אז יש לי סקריפט פייתון שמחשב את הסיסמה על פי ההאש:



למעשה הקלט יהיה הבתים והוא מחשב קסור של BE עם כל אחד מתווים ומדפיס את הסיסמה.

הנה הפלט של ההרצהתמונה שמכילה טקסט, מכשיר, מד, סגור

התיאור נוצר באופן אוטומטי

והסיסמה כשאני מריץ את זה

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

אגב מלהריץ עם עוד קלטים אני חושב שהסיסמה תלויה יותר באורך וגם שהיא תמיד עם הLEET בסוף וגם ההאש תמיד נראה דומה, אבל מצד שני המטרה שלי הייתה למצוא שם וסיסמה, ולמעשה אין טעם לחקור את קטעי הקוד המיותרים