מצאתי מנגנון אחד של אנטי דיבאג:

אחרי שהרצתי את התוכנית עם האנטי דיבאג כדי לנסות לראות איפה אני קורס ראיתי שאני מגיע לחלק הזה:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

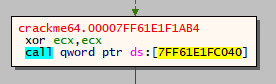
כמובן שהמשכתי להריץ וראיתי שאחרי כמה הרצות אני מגיע לצד שמאל וזה מקריס אותי כמו כאן:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיכמובן שאני לא רוצה לקרוס ולכן אפשרות אחת לנטרל את מנגנון האנטי דיבאג תהיה לבטל את הקריאה שיש שם לפונקציה או לבטל את הבדיקה וישר ללכת לצד ימין או כל אפשרות אחרת...

בכל מקרה הקוד כאן מעניין מכמה סיבות:

 דבר ראשון אנחנו לוקחים את הכתובת של היציאה מתהליך ושמים את זה בזיכרון במקום מסוים שנשתמש בהמשך.

 זה התמונה של צד ימין שאנחנו יוצאים, למעשה זה המקום שאליו אנחנו עלולים להגיע וזה די ברור שזה המקום הרע כי זה בדיוק איפה ששמרנו את הכתובת של יציאה מהתהליך.

עוד דבר מעניין שיש פה זה: תמונה שמכילה טקסט, מקורה, צילום מסך

התיאור נוצר באופן אוטומטי יש לנו כאן גם קוד ארוך יחסית שבודק את הבייט המסויים של EAX ואנחנו מריצים הרבה כתובות ומצביעים להגיע לשם.

למעשה אחרי שהרצתי את הקוד והסתכלתי על הערך של הרגיסטר ראיתי ש:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי כאן למעשה אפשר לראות שEAX שווה 1 שזה מחשיד כי הביט שאומר אם אנחנו בדיבא הוא גם 1.

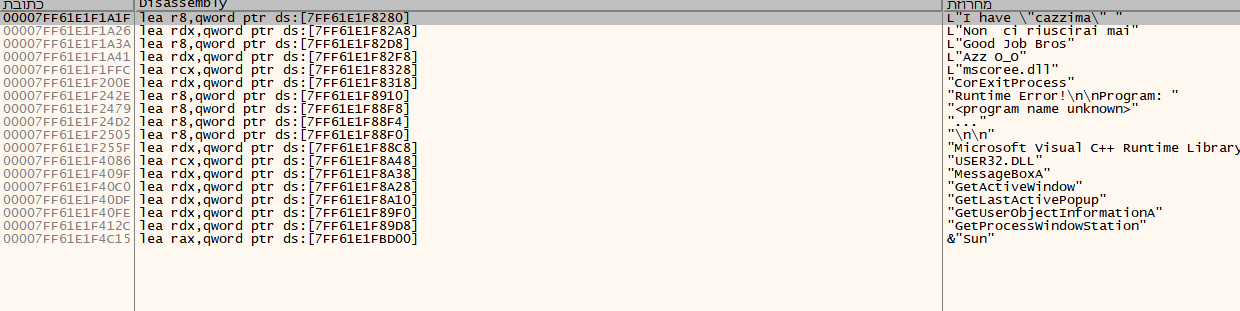
למעשה כל הגישה הארוכה הזאת לזיכרון כנראה אומרת לתוכנית אם אנחנו מדובגים, למעשה הפתרון שלי לפצ'פץ היא תהיה פשוט לדלג על הבדיקה ולקפוץ לצד הטוב: למשל:

תמונה שמכילה טקסט

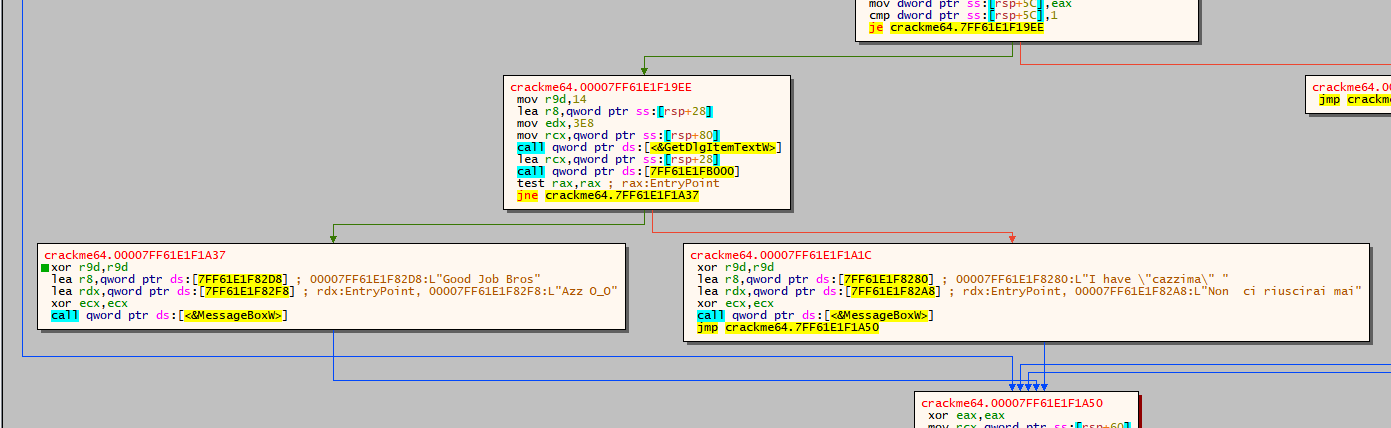
התיאור נוצר באופן אוטומטיוככה ייראה הקוד לאחר הפצ'פוץ'. למעשה אני הרווחתי שהקוד של האזור הטוב מיד אחרי התנאי אז במקום לשנות אותו לקפיצה לא מותנה שיניתי את זה שהוא לא יקפוץ בכלל ופשוט ימשיך לצד הטוב...

עכשיו אחרי שעשיתי את הפצ'פוץ' נשאר רק לעשות את הבדיקה של הגעה למסר הטוב:

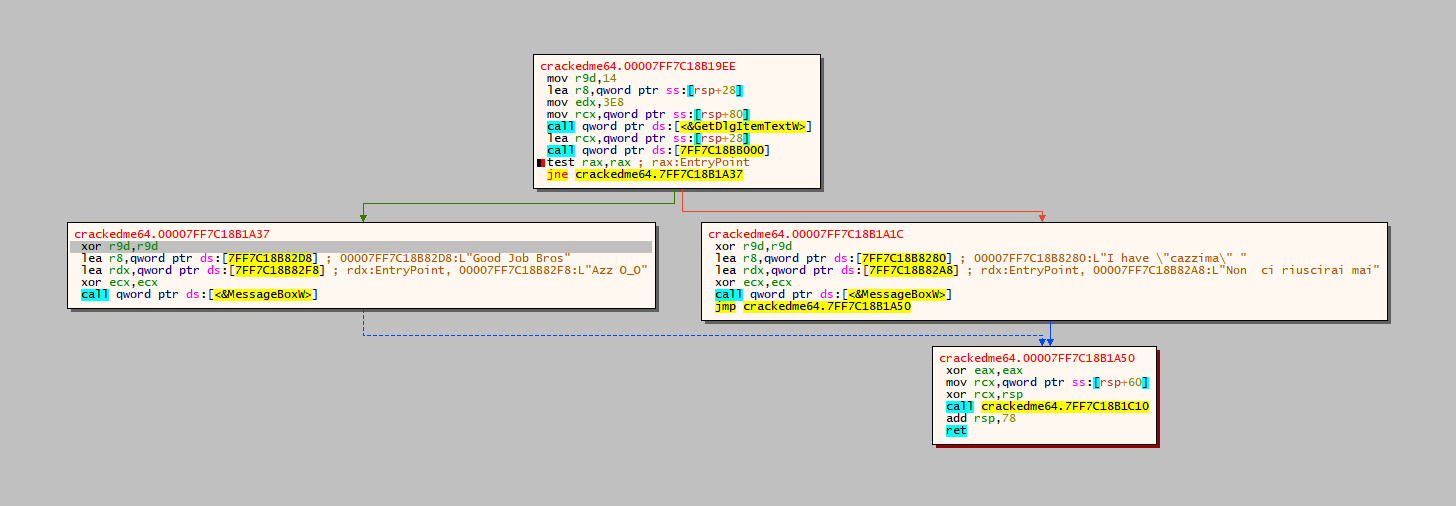
כדי להגיע למסר הטוב אני מתחיל עם בדיקה של המחרוזות שיש בקובץ בתקווה כמובן שהן לא מוצפנות, ואכן אני יכול לזהות כמה מחרוזות טובות:

כמובן שאני אתעניין באזור של ההודעה אם זה הצלחה או לא ובהודעה על כישלון(הרצתי את זה ואני יודע שהיא הטקסט המוזר למעלה, אבל בכל מקרה זה הטקסט היחיד פה)

אחרי שהלכתי למיקום שקיבלתי את הטקסט ובניתי את העץ המלא יצא שיש אזור שאני מעונין בו במיוחד:

למעשה די ברור שזה החלק שמעניין אותי להגיע לאזור של ההצלחה.

אני מעריך שבפונקציה לפני זה בודק את הסיסמה, אבל זה ממש לא מעניין אותי מה היא, אלא אני אפצ'פץ' את EIP כדי לקפוץ להדפסה של הסיסמה:

בשביל להגיע לאזור הטוב צריך שתודפס התיבה הראשונה קודם אז אני אעצור לפני הבדיקה אם זה סיסמה טובה או לא ואז אני אקפוץ למקום של ההדפסה של הצלחה:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי והנה המסר שהצלחתי! יאיי!

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיהקובץ אחרי הקפיצה.

ד"א כמובן שיש אינספורר דרכים לשנות את הקוד כך שיודפס הודעת הצלחה אבל הרבה זמן לא היה פתרון שכלל קפיצה עם EIP אז אני מנצל את זה בשביל זה.... כמובן שיש אפשרות לבטל את התנאי לבטל את הבדיקה של הסיסמה, לשנות את הבדיקה שתמיד תחזיר כאילו זה סיסמה טובה וכו'.

השלמות לשאלות שיש ותשובות מרוכזות:

מנגנוני האנטי דיבאג: היה בדיקה של הביט שאומר אם מדבגים אותנו, מחקתי את ההשוואה שהם עשו

איך מצאתי את המיין:

יש אפשרות עם IDA בדכ למצוא את זה בצורה פשוטה:

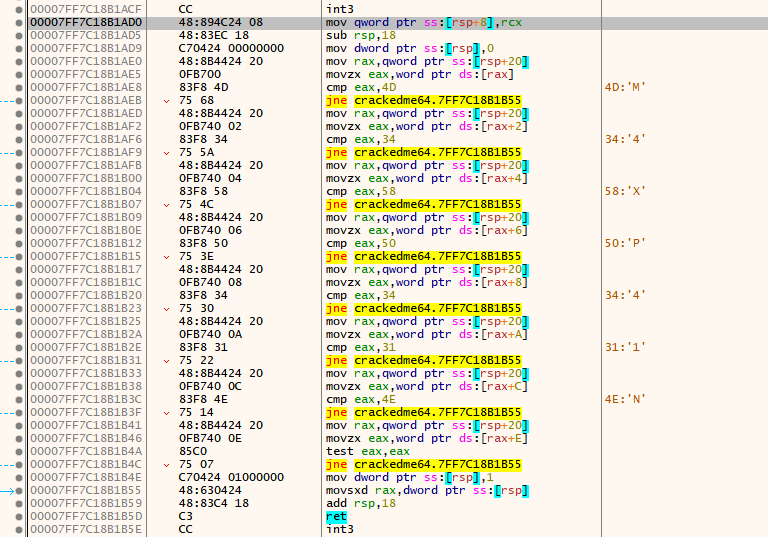
על פי IDA המיין נמצא כאן 00000001400018F0, איך שפתחתי את התוכנה זה ישר מביא את המיין:

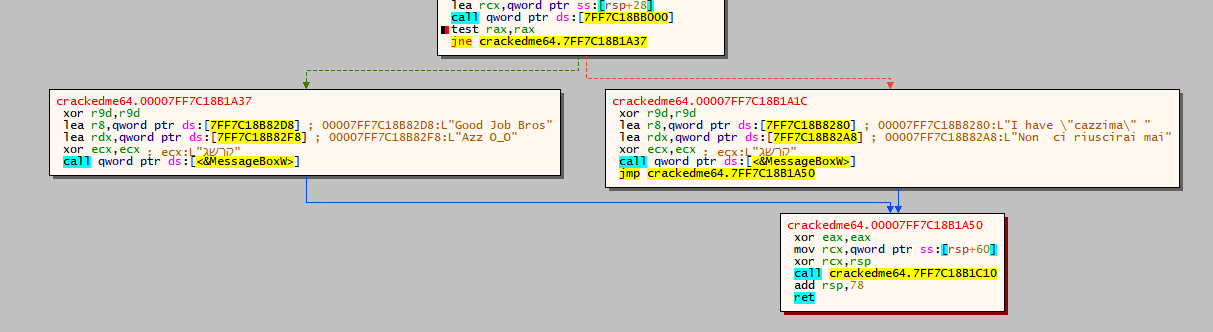
תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

האם רץ קוד לפני המיין: כן, אחרי הכל יש את הבדיקה של האנטי דיבאג לפני.

איפה בודקים את הסיסמה ואיך עקפתי:

זה הבדיקה של הסיסמה כמו שאפשר לראות שבודקים רגע לפני ההכרעה אם זה סיסמה טובה או לא:

השורה הראשונה שמודגשת בכחול זה הקריאה לבדיקה ואחריה בדיקה של הערך המוחזר.

איך עקפתי: פשוט שיניתי את EIP שיצביע על האזור הטוב, אפשרויות אחרות היו להעלים את הבדיקה וישר לקפוץ בלי תנאי לאזור הטוב.