***Anti-Ransomware***

**מסמך עיצוב**

**נועם אזולאי**



**הקדמה**

מטרת המסמך הזה היא תכנון מקדים של הפרויקט Anti-Ransomware. במסמך זה יתוארו המודולים, הפרוטוקולים והמבנה הכללי של המערכת.

קהל היעד של הפרויקט הינו כל אדם בעל מחשב אשר ברצונו להגן על המידע ומבלי להסתכן ליפול להונאת הRansomwares הקיימים, האפליקציה תפעל על כל מחשב מבוסס Windows.

Anti-Ransomware היא אפליקציה אשר תיתן לבעלי המחשב שברשותם מידע חשוב אופציה נוספת להגנה על המידע, ע"י מערכת מבוססת בשפת C, המערכת תציב "מלכודות" ובעזרתן יגלה ניסיונות להונאת המשתמש, במידה ויהיה חשד סביר לוירוס שכזה, המערכת תיידע את המשתמש ותשאל כיצד ירצה להגיב, האם לסגור את התוכנית או להמשיך.

הפעולות הניהוליות אשר יינתנו מהשרות הן:  
1. בדיקת שינויים בקבצי המלכודות.

2. הגדרת קבצי הרצה כמסוכנים או לא.

3. בדיקת שינויים ע"י תהליכים שונים והסדרתם כמסוכנים או לא.

מסמכים קודמים:

מסמך אפיון - <https://github.com/azoulaynoam/Anti-Ransomware/blob/master/Documentation/Project%20Proposal.docx>

הגדרות מושגים:

GUI – Graphic User Interface – מטרתו היא להציג למשתמש ממשק נוח לביצוע פעולות בסיסיות כמו הוספה לBlacklist/Whitelist.

Ransomware – וירוס אשר פעולתו העיקרית היא הצפנת קבצים טקסטואליים ובקשת תשלום מבעל המחשב על מנת לשחררם.

**מבט על**

המודולים של הDLL של C:

שכבת האינטרקציה עם מערכת ההפעלה – אחראי על שימוש בפעולות WINDOWS, שימוש בsysinternals.

שכבת ההפעלה – שכבה האחראית על ביצוע הפעולות המבוקשות ע"י הGUI.

המודולים של ה GUIב:C#

שכבת ההצגה – הgui יציג רשימות של קבצים, Blacklist וWhitelist, כאשר תוכנית חדשה תרוץ, והיא תתחיל בהצפנת קבצים, המערכת תזהה את הפעולה ותפסיק את התהליך, ומייד תציג הודעה למשתמש, האם ברצונו להוסיף את התהליך לBlack או Whitelist.

**פירוט רכיבי המערכת**