

**שם התלמיד: נועם אזולאי**

**ת"ז: 206824534**

**בית הספר: אורט גוטמן נתניה**

**שמות המורים: מיכאל צ'רנובילסקי וגד רוזנטל**

**מועד הגשה: 1/2016**

**מבוא**

וירוס הRansomware הוא וירוס שמטרתו היא רווחית, הווירוס פועל ע"י הצפנת המידע במחשב, ולאחר מכן הצגת הודעה בעלת התראה שהמחשב הוצפן, וכדי להחזירו לקדמותו יש לשלם סכום מסוים (כופר) ומכאן שמו.  
הווירוס יצפין קבצים עם סיומות מסוימות (לדוגמא txt, בדרך כלל קבצים טקסטואליים כי אלו הם אשר מכילים מידע חשוב, ובדרך כלל עם הצפנת RSA) ולאחר מכן יבקש דמי גבייה על שירות הDecryption, ויקציב זמן מסוים עד מחיקה מלאה של המידע.

המוטיבציה לפיתוח תוכנה שתתמודד עם הבעיה שתוארה לעיל מגיעה מהניסיון האישי שלי עם הווירוס, כאשר הייתי בכיתה ד הודבקתי באחת הגרסאות הראשונות שלו, וכפתרון פרמטתי את המחשב, היום כשיש לי כבר יותר ידע במחשבים אני יכול לפתח הגנה נגד אותו הווירוס, שזה יכול להיות מעניין. בנוסף לכך, אני אוהב לתכנת ומעניין אותי נושא ההצפות והווירוסים, ככה שמצאתי את הנושא המושלם.

התוכנה אמורה כביכול לבדוק כל תוכנה אשר ברצונה לקרוא מידע מקובץ, כאשר יוצבו במקומות ראשוניים (לדוגמא כונן C בתיקייה ששמה a יוצבו כמות מסוימת קבצי טקסט שמטרתם תהיה מלכודת לווירוס מסוג שכזה, ובמידה שהקבצים ישונו בצורה דרסטית ובמהירות לא אנושית, יהיה חשד לווירוס, ובמצב שכזה תהליך הווירוס יופסק, ותוצג הודעה על המסך שבה ייכתב שיש חשד לווירוס, והמשתמש יושאל האם ברצונו להמשיך בתוכנית או לא, משום שמצב כזה יכול להיות גם אצל מתכנים.

**תיאור המוצר**

המטרה המרכזית של המוצר היא הגנה מפני וירוס הRansomware אשר תהיה תחת שליטת המשתמש ולא כמו כל אנטי-וירוס מציק שיחסום גם במצב שזוהו רצון המשתמש, זהו הAnti-Ransomware.

התרחישים שהמערכת עונה עליהם הם זיהוי פעילות חשודה במחשב (שעלולה להעיד על Ransomware), והודעת המשתמש על התרחשות שכזאת ופתרונות אפשריים.

**אילוצים ודרישות**

הבעיות שהמערכת צריכה לדעת להתמודד איתן הן:

1. משתמש עלול לכתוב קוד אשר מטרתו היא הצפנת כמות קבצים אשר תעלה על חשדות הAnti-Ransomware.
2. Ransomware עלול להיות מוגן מפני הגנות שכאלו.
3. הRansomware עלול להספיק להצפין קבצים חשובים לפני שיגיע למלכודות, משום שסדר קריאת הקבצים משתנה (יכול להיות לפי גודל, לפי האלף בית, וכו').

היא נותנת להן מענה בכך ש:

1. המערכת תהיה בתפקוד מלא עם המשתמש וכל פעולה שהיא תבצע תבוצע רק עם אישור המשתמש.
2. המערכת צריכה לזהות Ransomwares שכאלה לפני הפעלתם.
3. יוצבו מלכודות לפי כל מני סדרות.

**תיחום הפרויקט**

הפרויקט עוסק בתקשורת מחשבים, בעבודה עם מערכת ההפעלה Windows ובאבטחת מידע.

המודולים שבהם המערכת משתמשת הם: הצבת מלכודות, בדיקת מלכודות, סגירת תהליכים, חסימת קבצי Execute, הוספת קבצים לWhitelist, הוספת קבצים לBlacklist.

**סביבת העבודה**

הפרוייקט ייכתב בPython וC#, כאשר כל התוכנית תכתב בPython והGUI בC#.  
סקריפט הPython יעבוד ע"י Process מהGUI ב C#ויתקשרו ע"י Pipe, כאשר קובץ כלשהו אשר הורץ ייחשד כRansomware תעלה הודעה על המסך האם ברצונו להמשיך את התוכנית או לחסום אותה, במידה וילחץ המשך, הקובץ יוסף לWhitelist, אחרת לBlacklist.

סביבות העבודה והכלים הנדרשים לפיתוח הם: notepad++ לכתיבת הקוד בPython, Visual Studio לכתיבת הקוד ב C#וVMWare לבדיקות.

**ניהול פרויקט עתידי**

|  |  |
| --- | --- |
| **יעדים** | **זמן ביצוע** |
| מחקר לגבי הרכיבים הנדרשים בשביל המערכת (קבלת מידע לגבי השימוש במשאבים של מחשב מרחוק, שליטה מרחוק בתהליכים וסגירתם, הגבלת שימוש במשאבים ועוד). | ינואר |
| הגשת מסמך עיצוב | ינואר |
| כתיבת קוד דימוי Ransomware (יקודד תיקיית קבצים בbase64) | ינואר |
| כתיבת מודול המציב מלכודות, ובודק אותם | פברואר |
| כתיבת מודול שסוגר תהליכים ע"י אישור מהמשתמש | פברואר |
| כתיבת מודול שיאפשר לתת הגדרות למערכת ויעבוד עם קבצי הגדרות (שבהם יהיה בין היתר ה- whitelist). | פברואר |
| כתיבת דו"ח ביניים. | סוף פברואר (הגשה ב-1 במרץ) |
| חיבור כל המודולים ביחד, בדיקות ותיקון שגיאות. | מרץ |
| כתיבת ה- GUI וחיבורו לחלק שנכתב ב- Python. | מרץ |
| עוד בדיקות ותיקון שגיאות. | מרץ + אפריל |
| כתיבת תיק הפרויקט. | אפריל |
| תוספות ושיפור הפרויקט. | אפריל + מאי |