****

**שם התלמיד: דוד קליין**

**ת"ז: 320774631**

**בית הספר: אורט גוטמן נתניה**

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

**מועד הגשה: 1/2016**

**מבוא**

כיום לחברות רבות מאוד חשוב להגן על האינטרסים שלהם, להגן על הסודות שלהם ואל המידע ששמור במחשבים שבחברה. לפעמים יהיה צורך למנוע מקבצים מסוימים לצאת מן הרשת הפנימית של החברה. פתרון אחד לבעיה זו הוא להיות מנותקים מן העולם החיצוני אך ברוב המקרים זהו לא פתרון פרקטי בגלל התלות שלנו באינטרנט, בשירותים שהוא מספק ובנוחיות שיש בו. כמו כן, גם את הרשת הפנימית אפשר לעקוף על ידי שימוש בUSB ואת זה אי אפשר "לבטל".

הרעיון שלי לפרויקט הוא לפתח פתרון חלופי, לפתח כלי אשר ימנע מאותם קבצים להגיע למקומות בלתי רצויים "ויצביע" על המחשבים אשר ניסו לגשת לקבצים אלו.

**תיאור המוצר**

המטרה המרכזית של העבודה היא ליצור כלי ימנע מהקבצים לא רצויים לעזוב את המחשב. הכלי יהפוך את המחשב לכספת מאובטחת אשר תודיע לבעלים שלה על נסיונות פריצה אליה. המוצר יהיה מחולק לשני חלקים עיקריים: שרת ולקוח.

השרת ינהל את כל הלקוחות שמותקנים על מחשבים שונים. הוא יגדיר לכל לקוח מה עליו לעשות, אילו סוגי קבצים לבדוק, באילו ישומים לבדוק שימוש בקבצים אלו ועל מה עליו לדווח ויקבל דיווחים מן הלקוחות על ניסיונות לבצע פעולות לא רצויות על אותם קבצים.

הלקוח שהוא התוכנה שתהיה מותקנת בכל מחשב ויהפוך את המחשב לכספת. הוא יבצע את כל הפעולות שהשרת יגדיר לו לבצע. חשוב להדגיש כי הלקוח נמצא על הגבול בין תוכנה שימושית לוירוס בגלל מה שהלקוח צריך לעשות בכדי שהוא יוכל לעקוב אחר שינויים בקבצים. על הלקוח לשנות את ההתנהגות של תוכנה או תוכנות (Hooking) במחשב כדי לברר אם הם מבצעות שימוש בקבצים מסוימים. בכדי לעשות זאת עליו להזריק DLL לתהליך של התוכנית שיבצא את הכל באופן אוטומטי. עם זאת התוכנה לא מבצעת שימוש לרעה במידע אשר היא מקבלת מאותם תוכנות. ברוב הזמן השינוי הוא פסיבי ורק כאשר יש צורך להתערב הלקוח יעשה זאת. יש לציין כי המטרה היא לאבטח את המחשב ולא להפך.

**אילוצים ודרישות**

בעיות/אירועים שהמערכת צריכה לדעת להתמודד איתם:

1. לאור העובדה שהמשתמש במחשב מודע לכך שהתוכנה מותקנת על המחשב, הוא יכול להיות מודע גם לדרך שבא התוכנית עובדת (מודיע על ניסיונות העברת הקבצים) ביכולתו לנסות "לתפוס" מידע זה, לשנות את תוכנו או למנוע ממנו להגיע אל היעד.
2. במקרה והמשתמש יכבה את התוכנית דרך מנהל המשימות או באופן ישיר המחשב יהיה לא מוגן וחסוף לדליפות מידע.

דרכי התמודדות עם הבעיות:

1. פרוטוקול התקשורת בין השרת ללקוח (התוכנית שעל המחשב) יהיה בנוי בצורה מתאימה כדי שלא יוכלו לחבל במידע בנוסף לכך המידע אשר נשלח יהיה מוצפן.
2. אחד הפתרונות למקרה בו המשתמש ינסה לסגור את התוכנית דרך מנהל המשימות היא להתקין את התוכנית כשירות (Service) על המחשב. ניתן להגדיר את השירות לאתחול אוטומטי.

**תיחום הפרויקט**

הפרויקט עוסק בשלושה נושאים עיקריים: תקשורת בין מחשבים, עבודה עם פעולות של מערכות הפעלה מסוג Windows ובהצפנה/אבטחת מידע העובר ברשת.

במערכת יהיו המודלים הבאים:

1. מודל לתקשורת בין השרת ללקוחות
2. מודל להצפנת מידע
3. מודל הכספת
4. מודל לחיבור בין הממשק הגרפי למוצר עצמו

**סביבת עבודה**

בפרויקט אני ישתמש בשני שני שפות תכנות: C++ לתכנות רוב הפרויקט וC# לתכנות הממשק הגרפי.

הערות:

השרת של הפרויקט ישתמש במסד נתונים (שיכול להשתנות בהמשך) אך לעכשיו אני אשתמש בMicrosoft Access.

הפרויקט כולו ייכתב בVisual Studio 2015.

**ניהול פרויקט עתידי**

|  |  |
| --- | --- |
| **יעד** | **זמן ביצוע** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |