

**עבודת גמר 5 יח"ל**

**נושא העבודה :** אנטי וירוס

**שם תלמיד :** ניק גלבוב

**ת.ז תלמיד :** **212616031**

**שם בית ספר ועיר :** קריית החינוך ע"ש עמוס דה-שליט, רחובות

**שם המנחה :** ערן בינט

**מועד הגשה :** 9.3.2018

תוכן עניינים

[1. מבוא 3](#_Toc509432052)

[2. תיאוריה 4](#_Toc509432053)

[3. תוצר סופי 5](#_Toc509432054)

[4. תהליך כתיבת הפרויקט 11](#_Toc509432055)

[5. מרכיבי פתרון 11](#_Toc509432056)

[6. תסריטי בדיקה 13](#_Toc509432057)

[7. רפלקציה 13](#_Toc509432058)

[8. הוראות התקנה ותפעול 14](#_Toc509432059)

[9. ביבליוגרפיה 14](#_Toc509432060)

[10. נספחים 14](#_Toc509432061)

1. מבוא
   1. נושא העבודה

נושא העבודה הוא אנטי וירוס.

* 1. מטרות מרכזיות

המטרות המרכזיות של העבודה הן:

* לזהות האם קיים חשד לוירוס בסיכויים גבוהים
* זמן ריצה יעיל
* GUI שמותאם למשתמש
* שליטה בThearding ביעילות (בשיטות הגילוי באנטי וירוס)
  1. רציונל

המוטיבציה שלי לפיתוח הרעיון הינה השליטה בקבצים, היכולת לחקור על קבצים זדוניים והיכולת לגלות מה עומד מאחורי הקובץ. הפרוייקט גורם לי לקרוא ולחקור על וירוסים ועל איך קבצים עובדים וזה מסקרן אותי.

* 1. קישור לחומר הנלמד

העבודה מתקשרת לחומר הנלמד במספר תחומים שונים. ראשית, בעבודה יש תקשורת בין מחשבים. יש תקשורת זדונית בין הוירוס להאקר, לשם שליטה ופתיחת פורט למחשב המותקף, יש תקשורת בין השרת ששולח קבצים לVM. שנית, אני משתמש בכלים של windows כגון פקודות של cmd, registry, task manager ומערכת הקבצים בשביל לגלות את התנהגות הוירוס . נוסף על כך, אני משתמש בתכנות מונחה עצמים כאשר אני מגלה אם נוסף קובץ למערכת או באחת משיטות הגילוי של הוירוס.

1. תיאוריה
   1. תיאוריה
   2. מוצרים קיימים

מערכת דומה הקיימת היום בשוק היאVirus total

הייחוד של המערכת שלי היא סריקה של הקובץ בתוך מכונה וירטואלית. סריקה זו מאפשרת גילוי חדש של וירוס שהחתימה שלו לא נשמרה במאגר של db (לדוגמה המאגר של virus total) .

ניתן לייצג את ההבדלים בטבלה:

|  |  |  |
| --- | --- | --- |
| טיפול בvirus | הפרוייקט שלי | Virus total |
| השוואת חתימות | V | V |
| גילוי וסריקה של וירוס חדש | V | X |

* 1. כשלים בפתרונות קיימים

?

1. תוצר סופי
   1. תיאור הפרויקט

המערכת הינה ...

המערכת מאפשרת מספר פעולות:

* לסרוק קובץ\תיקייה שהמשתמש בוחר ולבחור שהאנטי וירוס יוכל לרוץ ברקע על קבצים חדשים שנוספו למערכת.
* למשתמש תהייה אפשרות להסגיר את הוירוס ?-----שאלה לערן
* בדיקת email ?
  1. אלגוריתמים עיקריים

אלגוריתמים מרכזיים במערכת

1. אחד: האלגוריתם של סריקת הוירוס והמעקב אחרי שינויים שקרו

האלגוריתם אחראי על הרצת הוירוס כthread על מנת שירוץ ברקע יחד עם threading נוספים שיבדקו את השינויים המתחרשים ברקע לאחר הרצת הוירוס. השימוש בthread מאיץ את התהליך ובנוסף יכול להריץ פקודות cmd בלי block מהרצת הוירוס. הקושי שצריך לגרום לתוכנית לרוץ בזמן הריצה היעיל ביותר והקצר ביותר. לשם כך צריך תיזמון נכון בין הthreading והתייחסות לכל מיני מקרי קצה שיכולים להיות במהלך הרצת הוירוס. הכוונה במקרי קצה יכול להיות לדוגמה שהוירוס ניגש לקובץ ומהר מאוד סגר את הגישה שלו אליו כי השיג את מה שרצה מבלי לשנות שום דבר בקובץ ובאותו זמן האנטי וירוס לא הספיק להבחין בשינוי. באלגוריתם יש שימוש בlock של הפקודות של הcmd על מנת שפקודות לא יתנגשו ביניהם.

2. שתיים ?

* 1. ממשק משתמש
  2. תרחישים עיקריים

1. אחד
2. שתיים
3. תהליך כתיבת הפרויקט
   1. תהליך הפרויקט
   2. אתגרים ואופציות שונות למימוש
4. מרכיבי פתרון
   1. תיחום הפרויקט

* תקשורת – תקשורת בין המחשב שהמתקיף למחשב שמותקף על ידי הוירוס ותקשורת בין המחשב ששולח קבצים לסריקה לvm.
* אבטחת מידע -
* מערכת הפעלה – thearding, task manager, handle, cmd
* תצוגה – c# gui
* מבנה נתונים – תור- הקבצים שיהיו בblack list
* שימוש במחלקות ותיעוד של כל בלוק בקוד.
  1. סביבת העבודה (טכנולוגיה)
* שפות התכנות:

האפליקציה עצמה כתובה בpython ובc#

* סביבות פיתוח:

Idle, visual studio

* 1. מבט טופולוגי
  2. מבט מודולרי
  3. פירוט מודלים עיקריים

1. תסריטי בדיקה
   1. דגשים בבדיקה
   2. תסריטי בדיקה עיקריים
2. רפלקציה
   1. לוח זמנים מוערך לניהול הפרויקט:

|  |  |
| --- | --- |
| נובמבר | לממש אחת משיטות הגילוי של הוירוס ותכנן מה השיטות העתידיות |
| דצמבר | לממש את האבן דרך הראשונה ולשלב לפחות 3 שיטות+מכונה וירטואלית קובץ אחד שיריץ את הכל |
| ינואר | להתחיל לשלב עוד 2 שיטות גילוי+עבודה עם virus total |
| פברואר | עבודה על הgui + בניית הdb+יכולת לעשות black list |
| מרץ | המשך הgui |
| אפריל | תיקון באגים |

* 1. אתגרים ותרומה אישית
  2. תובנות

1. הוראות התקנה ותפעול
   1. תצורה ודרישות קדם
   2. התקנה
2. ביבליוגרפיה

במהלך כתיבת הפרויקט הסתמכתי על מספר מקורות מידע:

Stack overflow <https://stackoverflow.com/>-

Python web <https://www.python.org/>-

Handle <https://docs.microsoft.com/en-us/sysinternals/downloads/handle>

Virus total <https://www.virustotal.com/gui/home/upload>-

1. נספחים