**MalwareGuard**

מסמך עיצוב

V1.1

13.12.14

שי שוורץ

אבישג בניאשוילי

**הסטוריית גרסאות המסמך**

|  |  |  |  |
| --- | --- | --- | --- |
| **תאריך** | **עורך/ת** | **תיאור / תקציר השינויים** | **הערות נוספות** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **מבוא**

המסמך מיועד לאוכלוסייה בעלת רקע בסיסי בתכנות ובכתיבת קוד.  
נזקה - היא [תוכנה](http://he.wikipedia.org/wiki/%D7%AA%D7%95%D7%9B%D7%A0%D7%94) שמטרתה לחדור או להזיק ל[מחשב](http://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91) ללא ידיעתו של המשתמש בו – וירוס.

אפליקציה זדונית – אפליקציה אשר זוהתה כלא אמינה והתנהגותה לא תואמת לאופייה.  
אפליקציה חשודה – אפליקציה אשר חשודה כאפליקציה זדונית ויש חשש שהיא עלולה לגרום נזק.  
אפליקציה מאושרת – אפליקציה אשר זוהתה כאמינה, התנהגותה תואמת את אופייה.

סיווג – החלטה האם האפליקציה: זדונית, חשודה או מאושרת.

סריקה – בדיקה של כל האפליקציות המותקנות במכשיר על מנת לזהות נזקות.

[חתימה](http://he.wikipedia.org/w/index.php?title=%D7%97%D7%AA%D7%99%D7%9E%D7%94_(%D7%A7%D7%95%D7%91%D7%A5_%D7%9E%D7%97%D7%A9%D7%91)&action=edit&redlink=1) - מבנה הקובץ הייחודי לכל קובץ. בדומה ל[טביעת אצבע](http://he.wikipedia.org/wiki/%D7%98%D7%91%D7%99%D7%A2%D7%AA_%D7%90%D7%A6%D7%91%D7%A2) אצל בני אדם, כך גם חתימת הקובץ ייחודית לקובץ מסוים ברמת ודאות גבוהה.

התנהגות של תוכנה – התהליכים שמבצעת התוכנה, למשל שולחת מידע או כותבת מידע.

SQL - היא [שפת מחשב](http://he.wikipedia.org/wiki/%D7%A9%D7%A4%D7%AA_%D7%9E%D7%97%D7%A9%D7%91) [הצהרתית](http://he.wikipedia.org/wiki/%D7%AA%D7%9B%D7%A0%D7%95%D7%AA_%D7%94%D7%A6%D7%94%D7%A8%D7%AA%D7%99) לטיפול ועיבוד מידע ב[בסיסי נתונים יחסיים](http://he.wikipedia.org/wiki/%D7%9E%D7%A1%D7%93_%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D_%D7%99%D7%97%D7%A1%D7%99).

Java - היא שפת תכנות מונחית עצמים.

בסיס נתונים - הוא אמצעי המשמש לאחסון מסודר של[נתונים](http://he.wikipedia.org/wiki/%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D) ב[מחשב](http://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91), לשם אחזורם ועיבודם.

1. **ארכיטקטורת המערכת**
   1. **מבט על**

שרת – תפקיד השרת הוא להוות בסיס נתונים לחתימות והתנהגויות של נזקות מוכרות.  
לקוח – הלקוח הוא האפליקציה במכשיר המשתמש.

תקשורת שרת-לקוח:  
האפליקציה תבקש מהשרת את המידע השמור בו על מנת לבדוק האם קיימת באפליקציה מסוימת במכשיר נזקה כלשהיא.

אבטחה  
המידע בשרת הSQL יהיה מוצפן על מנת למנוע חדירה לשרת ושינוי המידע בו, ובכך להבטיח שלא נפגע מערך החתימות המיועד למנוע חדירת נזקות למכשיר.  
התקשורת בין השרת ללקוח תאובטח באבטחת PRIVTE-PUBLIC-KEY.

**קוד לקוח**

פונקציית התחברות :

פונקציה זו מופעלת פעם אחת בהפעלת האפליקציה. היא יוצרת קשר עם השרת ובודקת האם היה עדכון בחתימות במקרה שהיה שינוי היא קוראת ממנו ושומרת את המידע הנמצא בו. התקשורת עוברת על TCP.

מחלקת סיווג:

מחלקה זו אחראית על סריקת האפליקציות וסיווגן. המחלקה היא Public.

בנאי:

\*שדה "אפליקציה"-Private .שדה זה יכיל בתוכו את טעינת האפליקציה.

\*שדה "מצב"- Private.מאותחל לNULL(=לא עבר סיווג).

פונקציות:

\*"סיווג"- Private.פונקציה אשר עוברת על חתימת האפליקציה ותבדוק האם היא אמינה. אם הפונקציה נמצאה אמינה שדה "מצב" ישונה ל"Trusted".במקרה שהפונקציה נמצאה כ"חשודה" ,השדה "מצב" ישונה ל"Suspect".במידה ונמצאה כזדונית ,ישונה השדה ל"Malice".

\*"קבל מצב"- Public. פונקציה המחזירה את הערך של שדה "מצב".

GUI -  
ממשק משתמש אשר יאפשר את הפונקציות הבאות:  
"סריקת מכשיר"- לולאה אשר תעבור על כלל האפליקציות במכשיר, ותבצע עלייהן פונקציית "סיווג".  
אם ערך החזרה הוא "Suspect" האפליקציה תמוין לרשימה "Suspects" ותודפס למסך בסיום עבודת הפונקציה תחת הכותרת Suspects.  
למשתמש תהיה אפשרות להחליט מה לעשות עם האפליקציה שנמצאה כחשודה – "מחיקה" , "ויתור פעם אחת", "התעלמות".  
אם ערך ההחזרה הוא "Malice" האפליקציה תמוין לרשימה "Malicious" ותודפס למסך בסיום עבודת הפונקציה תחת הכותרת Malicious.  
למשתמש תהיה אפשרות להחליט מה לעשות עם האפליקציה הזדונית – "מחיקה" או "התעלמות".

אם ערך ההחזרה או "Trusted" לא יעשה דבר.

-"מחיקה" – פונקציה אשר תסיר את האפליקציה מהמכשיר.  
-"ויתור פעם אחת" – פונקציה אשר תשמור את האפליקציה כחשודה בתוך רשימה, ותישמר בהיסטוריית חשודים. פעם הבאה שתמצא האפליקציה כ"חשודה", תעלה כ"חשודה" ותסומן באות קלון של "נמצאה כחשודה בעבר".

-"התעלמות" – לא יעשה דבר.  
-"Quarantine"

**קוד שרת**

\*פונקציית התחברות-יוצרת קשר עם הלקוח ומעבירה לו את המידע המבוקש בצורה מאובטחת.

קוד של בסיס נתונים:

מטרתו לשמור בצורה מסודרת ומאובטחת חתימות של ווירוסים ידועים כדי להעבירן ללקוח.

אנחנו עדיין לא מכירים SQL , ולכן לא בטוחים איך הקוד ייכתב.

**אבטחה**

התקשורת בין השרת ללקוח תאובטח על ידי . SSL

ההתחברות לשרת תיעשה באופן מאובטח כדי שלא כל תוכנה תוכל לגשת לנתונים הנמצאים עליו(למשל וירוס שירצה לראות אם הוא מופיע ברשימה הידועה לשרת).

בנוסף לכך העברת המידע עצמו בין השרת ללקוח תעשה באופן מאובטח(מניעת MITM לדוגמה של וירוסים).

1. איזה מידע עובר במערכת?

-חתימות ווירוסים מוכרים יורדו לשרת הSQL מהאינטרנט ויישמרו שם. בעת התחברות האפליקציה לשרת ,תועבר רשימת החתימות לקובץ מוצפן .רשימה זו תשמש את האפליקציה לגלות נזקות במכשיר.

- חתימות האפליקציות במכשיר עוברות דרך המערכת לבדיקת "מצב"

- אפליקציות שסומנו כ"חשודות" וסומנו כ"ויתור פעם אחת" ישמרו בקובץ טקסט על המחשב (כדי לשמור היסטוריה של אפליקציה חשודה) באופן מוצפן

- לבדוק איזה מידע על האפליקציות שזקוק כדי לבחון את ההתנהגויות של אפליקציות חשודות

**ממשק גרפי:**

Scan Now

History

MalwareGuard

MalwareGuard

MalwareGuard

Malware name

File name

History

File name

Malware name

38%

Scan Now

Update Now

Options