**MalwareGuard**

מסמך אפיון

v1.0

1/12/2014

בניאשווילי אבישג  
שוורץ שי

**הסטוריית גרסאות המסמך**

|  |  |  |  |
| --- | --- | --- | --- |
| **תאריך** | **עורך/ת** | **תיאור / תקציר השינויים** | **הערות נוספות** |
| 1.12.2014 | כל הצוות | כתיבה ראשונה | O: |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. הקדמה

*MalwareGuard הינו אנטי וירוס ומלוור, הנועד להבין איזה פעולות* מתבצעות ע"י איזה אפליקציות והאם זה מתאים לאופי שלהן. ובכך לחסום אפליקציות זדוניות, לסמן אפליקציות חשודות ולאפשר למשתמש להחליט מה לעשות בנוגע לחשדות ולאשר אפליקציות נאמנות.

**1.1 מטרה**

*מטרת המוצר היא לשמור על בטחון מכשיר האנדרואיד של המשתמש מפני וירוסים ונוזקות שונות.*

* 1. **המוצר**
* *MalwareGuard*
* *MalwareGuard תצליח לזהות ניסיון חדירה למחשב של תוכנה זדונית טרם התקנתה, ובכך למנוע את האיום והנזק.*

*אם התוכנה הזדונית הייתה קיימת על המכשיר טרם התקנת MalwareGuard, המערכת תנסה לזהות את הווירוס בזמן פעולתו או לזהות את קיומו ולהתריע על כך למשתמש.*

**1.3 הגדרות**

*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.

1. **תיאור כללי**

**2.1 פונקציונליות**

*בדיקת אפליקציה חדשה – בכל פעם שהמשתמש ינסה להוריד אפליקציה חדשה למכשירו, האפליקציה תיסרק*

*ותעבור סיווג.*

*סריקת מכשיר – פונקציה אשר תסרוק את המכשיר ותחפש התנהגויות לא אופייניות.*

*הסטוריית סריקות – MalwareGuard תאפשר למשתמש לשמור את הסטוריית הסריקות שהתבצעו ולהתבונן*

*בה בכל זמן נתון.*

**2.2 מאפייני משתמשים**

*קהל היעד הינו משתמשי אנדרואיד מגרסה – XXX*.  
אין צורך ברקע טכנולוגי, האפליקציה תעבוד "מאחורי הקלעים" ולא תדרוש התערבות של המשתמש – מלבד אישור אפליקציות חשודות.

**2.3 אילוצים עיקריים**

זמן מעבד מינימלי.  
 מערכת אנדרואיד על המכשיר מגרסה – XXX ומעלה.

**2.4 הנחות ותלויות**

*המערכת תרוץ על מערכת הפעלה אנדרואיד.*

1. **דרישות מפורטות**

**3.1 דרישות של ממשקים חיצוניים:**

**3.1.1 ממשקי משתמש**:

GUI: ממשק משתמש אשר יאפשר לו לעשות סריקת מכשיר כשירצה או להסתכל על הסטוריית סריקות וחסימות.

**3.2 דרישות פונקציונליות**

בדיקת אפליקציה חדשה – MalwareGuard תבצע סריקה בכל פעם שהמשתמש יוריד אפליקציה חדשה, לאחר הסריקה האפליקציה תעבור סיווג.  
הפיצ'ר מקבל כקלט את האפליקציה החדשה, בודק את אופייה, ומבין האם היא עושה את מה שהיא אמורה לעשות – כלומר, האם היא פועלת על פי האופי שלה. בסיום הבדיקה, הפיצ'ר מחזיר כתשובה את התג שקיבלה האפליקציה לאחר סיווג – מאושרת \ חשודה \ חסומה.

סריקת מכשיר – MalwareGuard תבצע סריקה על כל האפליקציות המותקנות במכשיר ותחפש התנהגות לא אופיינית.  
הפיצ'ר לא מקבל קלט, יש גישה לכלל האפליקציות במכשיר , כל אפליקציה עוברת סריקה וסיווג, ומחזירה כתשובה את התג שקיבלה כל אפליקציה לאחר הסיווג - מאושרת \ חשודה \ חסומה.

**3.3 דרישות לא פונקציונליות**

*דרישות מהמערכת שלא מתבטאות בפיצ'ר ספציפי או בתהליך ספציפי שמתרחש במערכת אבל משפיעות על אופן עיצובה ומימושה, לדוגמא:*

**3.3.1** זמן מעבד קצר ככל האפשר.

**3.3.2 בתור אפליקציה שמטרתה למצוא רוגלות במכשיר המשתמש עלייה להיות נאמנה.**

**3.3.4 מסד נתונים מאובטחת, כתיבה מאובטחת לתוכו, וקריאה מאובטחת ממנו.**

**3.3.5 עדכוניים תקופתיים – חידוש מסד הנתונים, עדכון אופיין של אפליקציות.**

* 1. **דרישות בסיס נתונים:**
* *המידע ישמר בXML.*
* *מאגר טקסטואלי – לא נדרש נפח אחסון גבוה.*
* *רמת אבטחה גבוה.*