**Teurse מסמך עיצוב**

**פרטי התוכנה:**

תכנתים: גבי אברמוביץ , אלינה לוי , יעקוב טורצקי

שם התוכנה:Teurse

**תיאור**

הפרויקט  הוא סוס טרויאני שמושתל על מכשירים בעלי מערכת הפעלה אנדרואיד גרסאות 2.2 עד 4.3.1.

השרת הוא אתר שיש להתחבר אליו עם שם משתמש וסיסמא. דרך האתר ניתן לראות מידע שנאסף לגבי הלקוח וגם לאפשר שליחה של פקודות מהמשתמש לגבי שינוי מידע- לדוגמא שליחת אסמס, ביצוע שיחה, הוספת קובץ ועוד.

**מבני נתונים**

שרת

* טבלת אנשי קשר: מכילה את הרשומות הרלוונטיות (TBD) לכל איש קשר
* טבלת יומן שיחות: רשימת השיחות וההקלטות שלהם
* טבלת אודות הפלאפון
* טבלת SMS: מכילה מידע על כל SMS שנשלח או התקבל
* טבלת הגדרות המכשיר: מכילה רשימה של כל ההגדרות הקיימות במכשיר
* טבלת אירועים מלוח שנה: מכילה את כל האירועים הנמצאים בלוח השנה של המכשיר
* קובץ ובו רשימה של קבצים ותיקיות
* טבלת אפליקציות
* טבלה שמצביעה לרשימת קבצים + קבצים עצמם (יכווצו שישלחו)
* טבלת מיקומי GPS

לקוח

טבלאות

* טבלת אנשי קשר: מכילה את הרשומות הרלוונטיות (TBD) לכל איש קשר
* טבלת יומן שיחות: מכילה
* טבלת SMS: מכילה מידע על כל SMS שנשלח או התקבל
* טבלת אירועים מלוח שנה: מכילה את כל האירועים הנמצאים בלוח השנה של המכשיר
* טבלת אפליקציות
* טבלה שמצביעה לרשימת קבצים
* טבלת מיקומי GPS

קבצים

* קובץ ובו רשימה של קבצים ותיקיות

**לוגיקת תוכנית**

לקוח

* שליחת מידע: הלקוח ניגש אל כתובת הWEB של השרת (לדוגמא: evil-site.com/gateway.php?send) ושולח את המידע הרצוי
* קבלת מידע: הלקוח ניגש אל כתובת הWEB של השרת (לדוגמא: evil-site.com/gateway.php?receive) ומקבל את המידע הרצוי עפ"י הID שלו
* לאחר התקנה: בדיקת emulator – אם כן, השבתה של התוכנה, אם לא- נמשיך הלאה
* לאחר התקנה: במידה ויש גישה לאינטרנט- שליחת התרעה לאתר (בתוך ההתרעה יהיה מידע התחלתי – אודות הטלפון, מצב סוללה, מיקום gps).
* כל פעם שיש אינטרנט- שולחים מידע חדש לשרת ועדכון הטבלאות
* כיווץ כל המידע בטרם שליחתו (לשקול: המרת תמונות לרזולוציה נמוכה\הקלטות MP3 באיכות נמוכה)
* במידה והחיבור הופסק בעת העברת המידע- שליחה מחדש לאחר חידוש החיבור
* קריאת גיבויים מן הזיכרון של המכשיר
* Privilege Escalation: ע"י השגת ROOT או Device Administration

|  |  |
| --- | --- |
| **פרטי הפונקציה:** | **שם פונקציה:** |
| מבצע: שולח מידע לשרת | SendDataToServer() |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מקבל מידע מהשרת | ReicveDataFromServer() |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: שולח קובץ לשרת בצירוף מידע על הקובץ | SendFile(location, name, info) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: יוצר רשומה עם מידע חדש במסד הנתונים | SaveToDatabase(dbname, tablename, data) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: | GetFromDatabase(dbname, tablename, id) |
| מחזיר: את הרשומה המבוקשת |
| מבצע: מעדכן רשומה | UpdateRecordeInDatabase (dbname, tablename, id, data) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מוחק רשומה מהמסד | DeleteFromDatabase(dbname, tablename, id) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: בודק את מצב הפלאג בלופ | ListenToFlag(FlagName) |
| מחזיר: אמת במקרה והפלאג נדלק ושקר במקרה שהוא מכובה |
| מבצע: פונקציה רקורסיבית שעוברת על רשימת התיקיות והקבצים בתיקייה | GetFilesTree(dir) |
| מחזיר: רשימת תיקיות, תתי-תיקיות וקבצים במערך |
| מבצע: קורא קובץ | ReadFromFIle(location, name) |
| מחזיר: את ה-data שנמצא בקובץ |
| מבצע: יוצר קובץ חדש | AddFile(location, name) |
| מחזיר: אמת במקרה של הצלחה, שקר במקרה של כישלון |
| מבצע: כותב מידע לקובץ קיים (אם הקובץ לא קיים נקרא לפונקצייה Addfile | WriteToFile(location, name, data) |
| מחזיר: אמת במקרה של הצלחה,שקר במקרה של כישלון |
| מבצע: מוסיף תקייה | AddDir(location, name) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מוחק את תקייה | RemoveDir(location, name) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: שולח sms | SendSMS(phoneNumber,data) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מקליט שיחה | RecordCall() |
| מחזיר: אמת במקרה של הצלחה,שקר במקרה של כישלון |
| מבצע: | GetGpsInfo() |
| מחזיר: את פרטי המיקום של הלקוח |
| מבצע: | GetNetworkStat() |
| מחזיר: את סוג הרשת שהמשתמש מחובר אליה |

שרת

* המשתמש מתחבר לאתר
* האתר מציג לו מידע
* הצגת מידע עפ"י החשיבות שלו (פרמטרים מוגדרים מראש, תדירות השימוש וכו')
* מחיקת מידע מהלקוח
* שליחת מידע אל הלקוח (קבצים\תוכנות\פקודות לביצוע)
* מחיקת מידע מהשרת
* בקשת קובץ מן הלקוח

**אופן התקשורת בין השרת ללקוח:**

***חיבור בפעם הראשונה:***

לקוח

לקוח

שרת

שליחת פרטים בסיסים

הודעת אישור על קבלת המידע ושליחת סיסמא

הלקוח עובר לנוהל הרגיל

שליחת פרטים בסיסים- פרטים טכניים על המכשיר (מעבד , דגם ,RAM , גירסת מכשיר ומידע טכני על הסים).

הודעת אישור על קבלת המידע ושליחת סיסמא – השרת מודיע ללקוח שהוא קיבל את המידע והוא שולח לו סיסמא (כדי להתחבר עליו לשלוח גם את הסיסמא שלו וגם מידע בסיסי על המכשיר).

***נוהל רגיל:***

לקוח

שרת

לקוח

שליחת ה-ID והסיסמא

ZZZ

הודעת אישור

קבלת רשימת מטלות

שליחת מידע

שליחת ה-ID והסיסמא : הלקוח שולח לשרת את ה-HASH שהוא מחזרות עם כל המידע הבסיסי של המכשיר ובנוסף שולח לו סיסמא שאותה קיבל בחיבור הראשון.

הודעת אישור : השרת מאשר כי כל הפרטים נכונים ושיש חיבור בין השרת ללקוח.

קבלת רשימת מטלות :אם יש מטלות לביצוע הוא מבצע אותן.

שליחת מידע: הלקוח שולח מידע אל דף מסוים בשרת (כל מידע חדש שישנו בפלאפון הלקוח שולח לשרת).