**FOLLOWDUCKY / עבודה לשיפור ציון**

מסמך אפיון

יהונתן לחמן

<גרסה 1.0>

<28.12>

**היסטוריית גרסאות המסמך**

|  |  |  |
| --- | --- | --- |
| **תאריך** | גרסה | **תקציר השינויים** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**1. הקדמה**

1.1 מטרה

*המטרה של הפרויקט היא להשתיל מערכת מעקב למחשב של המותקף (לדוגמה שלי המורה בבית הספר) בעזרת זה להשיג שם משתמש וסיסמא של אתר ספציפי (במקרה שלנו וובטופ) ושיישלח לי את השם משתמש וסיסמא כך שתהיה לי גישה לזה.*

1.2 המוצר

*שם המוצר - FOLLOWDUCKY (השם לא סופי)*

* *בעזרת RUBER DUCKY אני משתיל תוכנת מסניף פקטות שתחכה שהמשתמש יכנס לאתר הרצוי. כאשר המשתמש נכנס לאתר, התוכנה מריצה keyloggger, שיעקב לאחר ההקלדה של השם משתמש וסיסמא ולאחר שהמשתמש יעבור לדף הכניסה לאחר הlogin התוכנה תשלח לי את המידע של הkeylogger אליי.*
* *לעומת דרכי התקפה אחרים, הFOLLOWDUCKY היא התקפה מהירה, כל מה שצריך בשביל להשתיל את התוכנה זה את המחשב של המותקף למשך כמה שניות. משם התוכנה תעשה את שלה ללא ידיעת המשתמש.*

1.3 הגדרות

*1) RUBBER DUCKY – מוצר שנראה כמו USB (דיסק און קי) אך במקום מקום לשמירה של קבצים, זה מדמה מקלדת חיצונית, והמקלדת הזו מריצה שורות של קוד בקצב מסחרר, והקוד הזה יכול לעשות כל מה שמקלדת רגילה יכולה.*

*2) keylogger – תוכנה שמטרתה לעקוב לאחר ההקלדות של המשתמש*

*3) Arduino (ארדואינו)– מיקרו בקר בעל מעגל מודפס יחיד, עם סביבת פיתוח ייחודית (הנקראת גם היא Arduino)*

*4) מסניף פקטות – תוכנה שמטרתה להאזין לכל התעבורה ברשת שהמשתמש של המחשב מנהל (כלומר אתרי האינטרנט שהוא גולש)*

*5) Ethical hacking – כידוע גם כ white hat, אלו פורצים עם מטרות טובות: אם הם פורצים לבדיקה ושכלול מערכות ההגנה, אם הם מטעם הממשלה ופורצים טרוריסטים, הם לא פורצים בשביל מטרות עצמאיות או בזמן עבירה על החוק.*

*6)DARKNET – רשת שאפשר לגשת רק באמצעות תוכנה. מה שמיוחד בה היא שהתקשורת אנונימית לחלוטין, כך שאי אפשר לדעת מי גולש. דבר זה יכול להוביל להאקרים ופושעים אחרים לגלוש ללא מעקב לאחר התכתבותם.*

*7) CMD – Command prompt, תוכנה שיש לכל מכשיר windows אשר בו אפשר לבצע כל פעולה שניתן לבצע באמצעות לעשות זאת בGUI (ממשק גרפי של משתמש)*

*8)* Github –  *אתר שבו אפשר להעלות קוד ולהוריד קוד ממשתמשים אחרים*

9) task manager – אפליקציה של windows שנותנת לראות את כל התהליכים והאפליקציות.

10) API – application programming interface – ערכה של ספריות קוד, פקודות, פונקציות ופרוצדורות מן המוכן, בהן יכולים המתכנתים לעשות שימוש פשוט, בלי להידרש לכתוב אותן בעצמם כדי שיוכלו להשתמש במידע של היישום שממנו הם רוצים להשתמש לטובת היישום שלהם.

11) Twillio – אפליקציה המאפשרת גישה לכל מיני דרכי תקשורת

1. תיאור כללי

2.1 פונקציונליות

**ההתקפה מחולקת לארבעה חלקים: חלק השתילה של התוכנה בעזרת ה** RUBBER DUCKY  **, חלק האזנה של הגלישה עד מציאת האתר, חלק המעקב לאחר המקלדת, וחלק השליחה של שם המשתמש והסיסמא.**

2.2 קהל היעד

**קהל היעד מחולק ל2: למקרה שאני עושה התקפה אטית (**Ethical hacking**) ומקרה בו אני מתקיף מטעמי אינטרסים אישיים. במקרה שאני מתקיף התקפה אטית, אני יכול להביא את המוצר למקומות כמו השב"כ והמוסד, בהם יכול להיות שימוש בהתקפה של ארגוני טרור וכניסה לאתר של הארגון. המקרה השני, בו אני מתקיף למטרות רווח עצמיות תוך התעלמות מהחוקים, יכולה בתיאוריה לשמש את כולם – כל מי שרוצה לפרוץ למחשב ולקבל סיסמא בכדי להיכנס ולעשות חלילה זדון לקורבן. בדוגמא שלי, בה אני מתקיף מחשב של מורה ומקבל שם משתמש וסיסמא של ה**webtop **בכדי להעלות את הציון שלי היא מטרה כזו.** למרות שאני עושה התקפת דוגמה מטעמי אינטרסים אישיים, זוהי רק הדגמה ואני לא מנצל את הפרויקט לפרוץ לאנשים למען רווח אישי. זהו רק סיפור כדי להדגים את הפוטנציאל של המוצר.

2.3 אילוצים עיקריים

**המחשב צריך להיות מחשב בגרסה של על** Windows 10 **בלבד (יכול להיות שגם על מוצרי** Windows **ישנים יותר, צריך לעשות בדיקות). ההתקפה דורשת מחשב בעל חיבור אינטרנטי, בכדי להוריד את התוכנה הדרושה והגעה לאתר האינטרנט הרצוי.**

2.4 הנחות ותלויות

**ההתקפה תרוץ בסביבת עבודה של** Windows

**2.5** סיקור מצב השוק כיום (אופציונלי)

כיום אין מוצר הדומה לשלי (אולי בשוק השחור או בDARKNET). אולי ישנן תוכנות זדוניות דומות, אך אין הן מפורסמות לציבור הרחב בשל פגיעה אפשרית במחשבים של אחרים. ממה שחיפשתי באינטרנט, אין התקפה של RUBBER DUCKY שעושה את מה שאני מתאר לעיל.

1. דרישות מפורטות

3.1 דרישות פונקציונליות

* USB RUBBER DUCKY *– בעצם אני משתמש בארדואינו, ומתכנת לתוך זה פעולות של מקלדת בשפת*

*ארדואינו. הפעולות העיקריות של המקלדת שהאדואינו צריך לבצע הן לגשת ל* cmd, *להוריד קובץ מאתר מסוים (כרגע זה אתר ב*github *, אבל זה יכול להיות מכל אתר) ולהריץ את התוכנה שירדה. לאחר מכן זה סוגר את ה* cmd, *ואפשר להוציא את הארדואינו.*

* *תוכנת מסנף פקטות – המטרה של התוכנה, לאחר שהיא מורצת תחילה בcmd היא לבסס את מקומה, כלומר לגרום לעצמה לרוץ כל פעם שהמשתמש נכנס למחשב. המטרה העיקרית של התוכנה – להאזין לגלישה של המשתמש, ולחכות עד שהוא נכנס לאתר היעד. כאשר זה קורה, התוכנה קוראת לkeylogger. החלק השני של המסניף פקטות הוא לבדוק מתי המשתמש עובר לאחר דף הכניסה (כך שהתוכנה תוכל לשלוח לי את השם משתמש והסיסמא שהיא תפסה).*
* *Keylogger – תפקידו, כאשר הוא נקרא ע"י המסניף פקטות, הוא להאזין לפעולות המקלדת, בכל שפה שתהיה, ולשמור את זה כך שיוכל לשלוח לי את ההקלדות.*
* *החלק האחרון בתוכנה הוא שליחת ה* SMS*. זה ייעשה ע"י קוד בתוכנה ששולח דרך* API *של* Twillio*לטלפון שלי. לאחר השליחה התוכנה תמחק את עצמה מהמחשב המותקף.*

3.3 דרישות לא פונקציונליות

**3.3.1 דרישות ביצועים (performance) – דרוש** RUBBER DUCKY  **לא יצטרך להיות תקוע במחשב יותר**

**מחצי דקה, אחרת זה יהיה חשוד.**

**3.3.2 דרישות מהימנות (reliability) – על התוכנה להסניף את כל הפקטות, אחרת התוכנה לא תדע מתי המשתמש נכנס לאתר הרצוי. בנוסף, התוכנה צריכה לעקוב לאחר כל האותיות שמוקלדות, כולל שינוי בשפה ואותיות גדולות וקטנות באנגלית, בכדי לדעת באופן הברור ביותר את הסיסמא ושם המשתמש.**

**3.3.3 דרישות זמינות (Availability) – עד השגת המטרה, התוכנה חייבת להיות מופעלת בכל עת. זה כולל גם מצבים בהם המשתמש מכבה ומדליק את המחשב.**

**3.3.4 דרישות אבטחה (security) – אין דרישות אבטחה לתוכנה.**

**3.3.6 דרישות ניידות (portability) – דרוש להיות ליד המחשב המותקף כדי להכניס לו את ה** RUBBER

DUCKY**, אחרת ההתקפה לא תוכל לצאת לפועל. התוכנה עובדת על כל מחשב** windows 10

1. **שלבים של הפרויקט**

**4 שלבים אפשריים נוספים בפרויקט**

שלב ראשון – שלב מינימלי, שמתואר על המוצר לעיל. בהנחה שהמשתמש הוא אדמין, אין לו סיסמא בכדי להפעיל cmd עם הרשאות של admin, אפילו ללא המחיקה של התוכנה מהמחשב או תחכומים נוספים. המקלדת תוריד את התוכנה, המשתמש מיד לאחר מכן יכניס שם משתמש וסיסמא והתוכנה תשלח לי.

שלב שני – צעד מתקדם יותר, התוכנה תמחק את עצמה, תגרום שתרוץ גם אם המשתמש מכבה את המחשב, אולי אפילו תעקוף הרשאות אדמין אם המשתמש לא אדמין. זה השלב שאני רוצה לעבור בסיום הפרויקט.

שלב שלישי – התוכנה תוכל להסוות את עצמה ואי אפשר יהיה לראות את זה תהליך או אפליקציה בtask manager. בנוסף לזה, אי אפשר יהיה למחוק את זה (אם ימחקו את המסניף פקטות, הkeylogger יוריד את זה מחדש, ולהפך). התוכנה תדע יותר מזה גם למחוק את המקום בו נשמר הזיכרון של השם משתמש והסיסמא לאתר, מה שיבטיח שהמשתמש יכניס את השם משתמש והסיסמא (התוכנה לא תעבוד אם האתר כבר זוכר אוטומטית את הנתונים של המשתמש והוא בסוף לא יקליד את הסיסמא).

שלב רביעי – ההתקפה לא מוגבלת למחשב המותקף, אלא תעביר את עצמה לכל המחשבים שנמצאים ברשת המקומית. בשלב הזה התוכנה תשוכלל לכך שתצליח לזהות אתר שמצריך סיסמא, תפעיל את הkeylogger ותשלח לי את השם משתמש והסיסמא.