**פרויקט בכופרה – 236349**

**FSD – File System Defender**

**דו"ח סיכום**

**אביב תשע"ח**

**מגישים:**

אלכסנדר גורביץ'

דניס סביש'וב

**מנחים:**

פרופ' אלי ביהם

אסף רוזנבאום

דר. ניר לבי

**תוכן עניינים**

* מבוא
* סקר
* הסבר על דיזיין
* נקודות בעיתיות
* פירוט הבדיקות
* הוראות לבנייה הפרויקט
* ביבליוגרפיה

**מבוא:**

במסגרת פרויקט זה פיתחנו אנטי וירוס נועד להגן מפני תוכנות כופר.

**תוכנת כופר**  היא נוזקה המגבילה גישה למערכות ה[מחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91) הנגוע בדרך מסוימת, ומשמשת ל[סחוט](https://he.wikipedia.org/wiki/%D7%A1%D7%97%D7%99%D7%98%D7%94_(%D7%A2%D7%91%D7%99%D7%A8%D7%94)) מה[משתמש](https://he.wikipedia.org/wiki/%D7%9E%D7%A9%D7%AA%D7%9E%D7%A9_(%D7%9E%D7%97%D7%A9%D7%95%D7%91)) תשלום כסף על מנת שתוסר מגבלת הגישה [1].

**הסבר על דיזין:**

* **Kernel Mode**

בחלק ראשון של הפרויקט מימשנו Minifilter Driver.

Minifilter driver מתחבר לערימת מערכת קבצים בעזרת Filter Manager כדי לקבל I/O Operations מסוימים. זה נותן לנו מידע על מה הולך במערכת קבצים שלנו ובפרט בתיקייה ש user בחר להגנה, אחר כך Minifilter מעביר מידע הזו לאפלקציה ב User mode לניתוח הבא ועל סמכם נחליט האם process זדוני או לא.

בחרנו לקבל IRP’s(I/O Request Packet) מסוג READ, WRITE, CREATE, CLOSE, CLEANUP ,SET\_INFORMATION שזה IRP’s עיקרים.

בחרנו READ ו- WRITE IRP’s בגלל שזה שני פעולות עיקריות שבעזרתם עובד כופרה. אנו מחשבים אנטרופיה של כל פעולה כזאות כדי להבין כמה מידע שקוראים\כותבים היא מסודרת. לכתיבה\קריאה של מידע מוצפנת יהיה אנטרופיה גבוהה מאוד.

CREATE IRP נותן לנו מידע על זה שתהליך מסוים פותח או יוצר קובץ חדש וגם יש אופציה לפתוח קובץ כך שיהוסר בסגירה.

SET\_INFORMATION IRP עוזר לנו להבין מתי תהליך רוצה להסיר קובץ או לשנות שם של הקובץ או להעתיק קובץ למקום אחר שזה פעולות נפוצות של כופרה.

CLEANUP, CLOSE IRP’s מיוצרים בזמן סגירת קובץ ובזמן הזה אנו נרצה להשוות כמה קובץ השתנה לאחר עבודה עמו.

Minifilter מעביר מידע לאפלקציה ב user mode כמו סוג של IRP, ID של תהליך, נתיב לקובץ, אנטרופיה של קריאה\כתיבה, שם חדש של קובץ אם הוא השתנה.

* **User Mode**

מימשנו אפלקציה שמקבלת מידע על IRP’s מקרנל ובעזרתה עושה ניתוח של תהליך ומחליטה האם תהליך זדוני. משתמש יכול לבחור תיקייה להגנה, להרוג תהליך מסוים, לשנות אופן פעולה.

משתמש יכול לבחור תיקייה להגנה ואפליקציה שולחת הודעה לקרנל ומנקודה הזאת Minifilter יסנן רק IRP רלוונטים.

בהתאם לקובץ ול PID(Process ID) מוסיפים אותם למבנה נתונים שאוסף תהליכים וקבצים רלוונטים. תלוי בסוג של IRP אנו מעדכנים סטטיסטיקוט של קבצים ותהליכים:

WRITE, READ IRP’s – אנו מעדכנים אנטרופיה ממוצעת ומספר בתים של קריאה\כתיבה.

CREATE IRP – מחשבים ערך התחלתי של הקובץ לחישוב אחר כך ערך שינוי של הקובץ.

SET INFORMATION IRP – בודקים האם תהליך רוצה להסיר את הקובץ או שתהליך השתנה שם של הקובץ ומעדכנים שם במבנה נתונים שלנו. גם בנקודה הזאת אנו בודקים האם סיומת של הקובץ השתנתה ואם תהליך מעביר קובץ מתיקייה הוגנת או שמכניס קובץ חדש בפנים או מחליף קובצ קיים.

CLEANUP, CLOSE IRP’s – אם פתחנו קובץ עם אופציה הרסה בסגירתו או שתהליך ביקש להסיר קובץ בודקים האם קובץ נמחק. אחרת בודקים כמה השתנה קובץ אחרי פעולות של תהליך.

בסוף ניתוח IRP ועידכון סטטיסטיקה אנו בודקים triggers שביחד מראים האם תהליך זדוני או לא. מימשנו כמה triggers:

-Entropy Trigger : מסתכלים על הפרש בין אנטרופיות ממוצעות של כתיבה וקריאה

File Distance Trigger- : יחס בין מספר פעמים שתהליך עבר סף LZJ distance אחרי שינוי בקובץ לסה"כ פעמים שתהליך שינה את הקובץ

* File Extension Trigger :
* Deletion Trigger : יחס בין מספר קבצים שתהליך מחק או העביר
* Rename Trigger
* Access Type Trigger
* Move In Trigger
* Change Extension Trigger
* High Entropy Replace Trigger

כש מקבלים יותר מ 5 triggers תלוי באופן פעולה אנו הורגים תהליך או שרק מודיעים למשתמש שזיהינו תהליך חשוד.

**נקודות בעיתיות:**

**פירוט הבדיקות:**

**הוראות לבנייה הפרויקט:**

**ביבליוגרפיה:**

[1] <https://he.wikipedia.org/wiki/%D7%AA%D7%95%D7%9B%D7%A0%D7%AA_%D7%9B%D7%95%D7%A4%D7%A8>